VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ VE SPOLEČNOSTI VYVÍJEJÍCÍ SOFTWARE

PROPOSAL FOR THE IMPLEMENTATION OF SECURITY MEASURES IN THE SOFTWARE DEVELOPMENT COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Daniel Štěpánek**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Daniel Štěpánek**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh zavedení bezpečnostních opatření ve společnosti vyvíjející software

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je návrh zavedení bezpečnostních opatření pro zvládání největších rizik a zvýšení informační bezpečnosti ve společnosti vyvíjející software.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

L. S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
ředitel	děkan

ABSTRAKT

Diplomová práce se zaměřuje na návrh zavedení bezpečnostních opatření ve společnosti vyvíjející software. V teoretické části jsou definovány vybrané pojmy v oblasti informační bezpečnosti. Analytická část řeší analýzu a zhodnocení současného stavu bezpečnosti ve společnosti. Vlastní návrh řešení obsahuje analýzu rizik, návrh opatření pro zvládání rizik a ekonomické zhodnocení.

ABSTRACT

Master's thesis focuses on proposal for the implementation of security measures in the software development company. Theoretical section defines chosen information security terms. Analytical section deals with analysis and assessment of current security situation in the company. Solution proposal contains risk analysis, proposal of security measures for risk treatment and economic evaluation.

KLÍČOVÁ SLOVA

informační bezpečnost, aktivum, hrozba, zranitelnost, riziko, analýza rizik, bezpečnostní opatření, ISO/IEC 27001, ISO/IEC 27002

KEYWORDS

information security, asset, threat, vulnerability, risk, risk analysis, security measures, ISO/IEC 27001, ISO/IEC 27002

BIBLIOGRAFICKÁ CITACE

ŠTĚPÁNEK, D. *Návrh zavedení bezpečnostních opatření ve společnosti vyvíjející software*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 116 s. Vedoucí diplomové práce Ing. Petr Sedlák.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 22. května 2017

…….

PODĚKOVÁNÍ

Tímto děkuji Ing. Petru Sedlákovi za ochotu, čas a cenné připomínky při tvorbě diplomové práce. Dále děkuji vedení společnosti a kolegům za spolupráci.

OBSAH

ÚVOD 11
1 CÍLE PRÁCE 12
2 TEORETICKÁ VÝCHODISKA 13
2.1 Základní pojmy 13
2.2 Podnikové procesy 16
2.3 Demingův cyklus (PDCA) 17
2.4 Řízení informačních technologií a bezpečnosti informací 19
2.4.1 Koncepce řízení 19
2.4.2 Rámce a metodiky 20
2.5 Normalizační instituce 23
2.6 Normy 24
2.7 Systém řízení bezpečnosti informací (ISMS) 26
2.7.1 Etapy zavádění ISMS 27
2.7.2 Povinná dokumentace 29
2.7.3 Budování bezpečnostního povědomí 30
2.8 Aktiva 32
2.9 Rizika 32
2.10 Opatření 32
3 ANALÝZA SOUČASNÉHO STAVU 34
3.1 Představení společnosti 34
3.2 Podnikové procesy 34
3.3 Současný stav bezpečnosti 38
3.3.1 Bezpečnostní politika a organizace bezpečnosti informací 38
3.3.2 Řízení aktiv 39
3.3.3 Bezpečnost lidských zdrojů a řízení přístupu 39

3.3.4 Fyzická bezpečnost a bezpečnost prostředí 40
3.3.5 Řízení komunikací a řízení provozu 40
3.3.6 Zvládání bezpečnostních incidentů 42
3.4 Zhodnocení současného stavu 42
3.5 Očekávání a východiska vedení 43
3.6 Analýza konkurenčního prostředí 43
4 VLASTNÍ NÁVRH ŘEŠENÍ 44
4.1 Rozsah a hranice 44
4.2 Analýza rizik 44
4.2.1 Identifikace a ohodnocení aktiv 44
4.2.2 Identifikace hrozeb a zranitelností 46
4.2.3 Identifikace rizik 49
4.2.4 Vyhodnocení analýzy rizik 51
4.3 Akceptace rizik 51
4.4 Návrh opatření pro zvládání rizik 53
4.4.1 A.6 Organizace bezpečnosti informací 54
4.4.2 A.7 Bezpečnost lidských zdrojů 58
4.4.3 A.8 Řízení aktiv 60
4.4.4 A.9 Řízení přístupu 61
4.4.5 A.10 Kryptografie 63
4.4.6 A.11 Fyzická bezpečnost a bezpečnost prostředí 65
4.4.7 A.12 Bezpečnost provozu 68
4.5 Aplikovatelnost navržených opatření 72
4.6 Obecné nařízení o ochraně osobních údajů 74
4.7 Údržba, přezkoumání, zlepšování 75
4.8 Ekonomické zhodnocení a časový plán 76

4.8.1 Náklady na návrh opatření 76
4.8.2 Náklady na zavedení (údržbu) opatření (první etapa) 77
4.8.3 Celkové náklady na návrh a zavedení opatření (první etapa) 78
4.8.4 Časová náročnost zavedení bezpečnostních opatření (první etapa) 78
5 ZHODNOCENÍ A PŘÍNOSY PRÁCE 79
ZÁVĚR 80
SEZNAM POUŽITÉ LITERATURY 82
SEZNAM ZKRATEK 84
SEZNAM TABULEK 85
SEZNAM OBRÁZKŮ 86
SEZNAM PŘÍLOH 87

ÚVOD

V teoretické části se budu zabývat pojmy z oblasti bezpečnosti informací, např. aktivy, riziky, opatřeními, koncepcemi řízení bezpečnosti informací, rámci, metodikami, normalizačními institucemi, normami nebo systémem řízení bezpečnosti informací.

V analýze současného stavu přiblížím společnost, pro kterou návrh zavedení bezpečnostních opatření zpracovávám. Představím společnost, nastíním její hlavní podnikové procesy, analyzuji současný stav bezpečnosti a kriticky jej zhodnotím.

Ve vlastním návrhu řešení vypracuji analýzu rizik. Některá rizika budu akceptovat, u některých navrhnu opatření pro jejich zvládání. Navržená bezpečnostní opatření detailně popíšu a nastíním jejich implementaci. Odhadnu časovou náročnost a náklady na implementaci jednotlivých opatření. Návrh a zavedení bezpečnostních opatření ekonomicky zhodnotím. Vyčíslím časovou náročnost a náklady na návrh opatření. Odhadnu časovou náročnost a náklady na zavedení opatření a jejich pravidelnou údržbu. Vyčíslím částku, která je pro návrh a zavedení opatření pro zvládání rizik potřebná.

Zhodnotím přínosy práce, splnění cílů práce a očekávání vedení společnosti.

1 CÍLE PRÁCE

Cílem práce je návrh zavedení bezpečnostních opatření pro zvládání největších rizik a zvýšení informační bezpečnosti ve společnosti vyvíjející software.

Pro splnění cílů diplomové práce je potřeba splnit následující části:

- teoretická východiska,
- analýza současného stavu,
- identifikace a ohodnocení aktiv,
- analýza rizik,
- návrh bezpečnostních opatření pro zvládání největších rizik.

Cílem práce není navrhnout komplexní řešení informační bezpečnosti, ale navrhnout zavedení vhodných bezpečnostních opatření na základě analýzy rizik, požadavků vedení společnosti a dostupných zdrojů podniku (např. finančních, personálních, časových).

2 TEORETICKÁ VÝCHODISKA

2.1 Základní pojmy

V této kapitole obecně přiblížím některé pojmy a názvosloví, na které budu v praktické části navazovat.

Informační management

Souhrn činností, které vedou ke splnění cílů zpracováním dat v organizaci a jejich vytvářením. Zahrnuje všechny úlohy managementu (vedení, plánování, kontrolu), které se týkají získání, zpracování, přenosu a uložení informací. [1]

Současné pojetí informační managementu lze charakterizovat jako vědomý proces, při němž jsou shromažďována data, která jsou využívána pro podporu rozhodovacích a řídících procesů na všech úrovních řízení organizace. [1]

Data

Data (nebo také údaje) jsou statická fakta, která jsou časově nezávislá. Odrážejí stav reality a nelze je měnit. Můžou být získána např. pozorováním, výpočtem nebo měřením. Lze je chápat jako vyjádření faktů a poznatků ve formě vhodné k dalšímu zpracování. [1]

Informace

Význam přisouzený datům (získaný např. zpracováním, analýzou nebo prezentací dat) ve formě vhodné pro rozhodovací proces. Informace je subjektivní pojem, který je vázán na jejího příjemce, z čehož vyplývá, že pojem informace není jednoznačný. Informace jsou na rozdíl od dat výsledkem určitého procesu jejich zpracování. [1]

Informace představují aktivum, které je stejně jako další důležitá aktiva organizace podstatné pro činnost organizace a vyžaduje odpovídající ochranu. Informace mohou být uchovávány v mnoha formách, a to v digitální formě, v materiální formě, nebo jako nevyjádřené informace ve formě znalostí zaměstnanců. Informace nebo prostředky, které jsou přenášeny, ať jsou v jakékoliv formě, vyžadují vždy přiměřenou ochranu. [2]

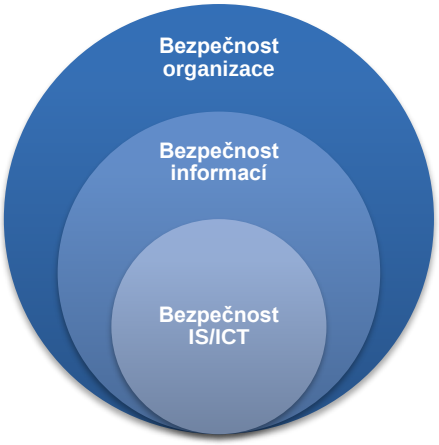
Informační systém

Soubor lidských zdrojů, technických prostředků a metod zabezpečujících sběr, přenos, uchování a zpracování dat za účelem tvorby a prezentace informací pro potřeby uživatelů.

Obecně lze informační systém chápat jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují. [1]

Bezpečnost organizace

Skládá se z bezpečností informací a bezpečnosti IS/ICT, které jí jsou podřízené.



Obrázek 1: Vztah úrovní bezpečnosti v organizaci (Upraveno dle [3])

Cílem bezpečnosti organizace je zajištění bezpečnosti objektů a majetku organizace (např. řízením, resp. omezením fyzického přístupu), čímž je do jisté míry zajištěna také bezpečnost informací a IS/ICT, které obsahuje. [3] [4]

Bezpečnost informací

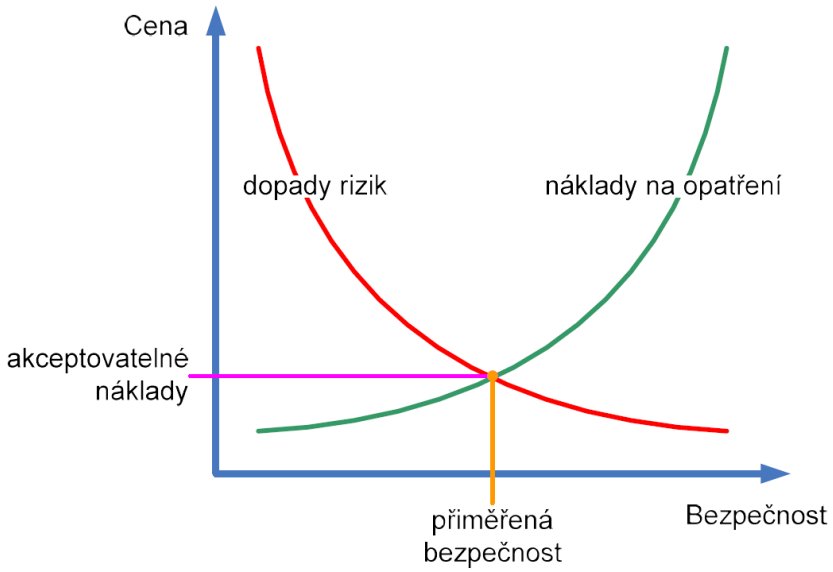
Cílem bezpečnosti informací je stanovit zásady nakládání s informacemi a způsob jejich ochrany. Bezpečnost informací v sobě zahrnuje bezpečnost IS/ICT (jak je patrné z obrázku výše), ale na rozdíl od bezpečnosti IS/ICT se bezpečnost informací zabývá také např. správou nedigitálních dat, způsobem zpracování dat nebo zásadami pro bezpečné zničení materiálů. [3]

Bezpečnost IS/ICT

Cílem bezpečnosti IS/ICT je chránit aktiva, která jsou součástí informačního systému společnosti podporovaného informačními a komunikačními technologiemi. [3]

Přiměřená bezpečnost

Přiměřenou bezpečností je stav, kdy investice a úsilí vynaložené na bezpečnost odpovídají hodnotě aktiv a míře možných rizik. [4]



Obrázek 2: Graf přiměřené bezpečnosti za akceptovatelné náklady (Převzato z [4])

Důvěrnost

Vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům. [2]

Integrita

Vlastnost přesnosti a úplnosti. [2]

Dostupnost

Přístupnost a použitelnost na žádost oprávněné entity. [2]

Aktivum

Cokoliv, co má pro organizaci nějakou hodnotu. Může se jednat jak o hmotný, tak nehmotný majetek. [4]

Hrozba

Událost ohrožující bezpečnost zneužitím zranitelnosti, jejíž působením může dojít k poškození nebo zničení aktiva. [4]

Zranitelnost

Slabé místo aktiva nebo opatření, které může být využito hrozbou. [3] [4]

Riziko

Pravděpodobnost (míra) ohrožení aktiva, která vzniká kombinací hrozby a zranitelnosti aktiva. [1] [4]

Dopad

Poškození nebo zničení aktiva v důsledku působení hrozby. [3] [4]

Opatření

Aktivita umožňující snížení nebo úplné odstranění hrozby. [3] [4]

Bezpečnostní událost

Zjištěný výskyt stavu systému, služby nebo sítě označující možné narušení politiky bezpečnosti informací nebo selhání opatření; nebo předem neznámá situace, která může být pro bezpečnost závažná. [2]

Bezpečnostní incident

Jednotlivá nežádoucí nebo neočekávaná událost bezpečnosti informací nebo série nežádoucích nebo neočekávaných událostí bezpečnosti informací, které mohou s významnou pravděpodobností vyvolat kompromitování operací souvisejících s činností organizace a ohrožení bezpečnosti informací. [2]

Standard

Dokumentovaná úmluva obsahující technické specifikace nebo jiná přesně stanovená kritéria používaná jako pravidla nebo směrnice. Velmi často jsou nástrojem dynamického prosazování technické politiky a následného pokroku. [4]

Norma

Doporučení použitelných standardů k realizaci požadovaného kompatibilního řešení. V oblasti ICT se jedná o předpisy nebo směrnice vydávané různými konsorcii uživatelů nebo výrobců, které jsou velmi často výsledkem těžce dosaženého kompromisu. [4]

2.2 Podnikové procesy

Proces je soubor vzájemně provázaných nebo vzájemně působících činností, které využívají vstupy pro dosažení zamýšleného výsledku. [5]

Podnikové procesy lze rozdělit do tří kategorií [6]:

- **Řídící procesy** – zabezpečují rozvoj a řízení výkonu společnosti a vytvářejí podmínky pro fungování ostatních procesů.
- **Hlavní procesy** – vytvářejí hodnotu v podobě výrobku nebo služby pro externího zákazníka, jsou tedy součástí hodnototvorného řetězce organizace.
- **Podpůrné procesy** – zajišťují podmínky pro fungování ostatních procesů tím, že jim dodávají hmotné i nehmotné výstupy, přitom ale nejsou součástí hodnototvorného řetězce.

2.3 Demingův cyklus (PDCA)

Metoda, při které dochází k postupnému zlepšování například kvality výrobků, služeb, procesů, aplikací nebo dat opakováním čtyř základních činností [4]:

- Plan (Plánuj)
- Do (Dělej)
- Check (Kontroluj)
- Act (Jednej)

Ustanovení ISMS (plánuj)

Etapa začíná určením rozsahu ISMS, který ovlivňuje politiku ISMS a aktiva, která jsou do ISMS zahrnuta. Dále jsou určena rizika ISMS, která vyjadřují, do jaké míry jsme schopni potřebám ISMS vyhovět. Jedním z posledních kroků této etapy je zajištění souhlasu vedení organizace s výběrem opatření a se zbytkovými riziky. Etapa většinou končí vypracováním prohlášení o aplikovatelnosti. [3]

Zavádění a provozování ISMS (dělej)

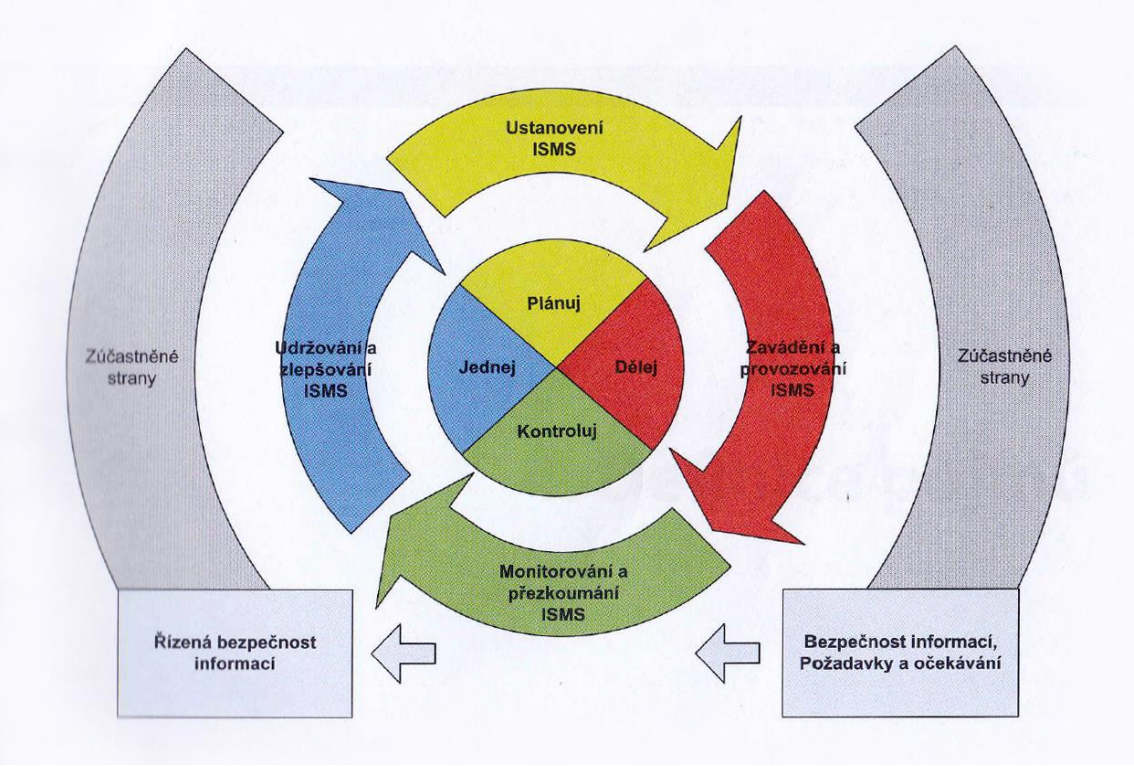
Etapa se soustředí na prosazení bezpečnostních opatření tak, jak byla navržena v předchozí etapě. Všechna bezpečnostních opatření by měla být uvedena v tzv. příručce bezpečnosti informací. Vytváří se plán zvládání rizik, zavádí se bezpečnostní opatření, definuje se plán pro budování bezpečnostního povědomí, upřesňují se způsoby měření a sledování účinnosti bezpečnostních opatření a vytváří se postupy pro zvládání bezpečnostních incidentů. [3]

Monitorování a přezkoumávání ISMS (kontroluj)

Cílem této etapy je zajištění účinné zpětné vazby. Účelem použitých zpětných vazeb je zajištění dostatku podkladů o skutečném fungování ISMS, které budou předloženy vedení organizace za účelem přezkoumání, zda aktuální stav ISMS odpovídá potřebám organizace. V této etapě tedy probíhá monitorování a ověřování účinnosti nasazených bezpečnostních opatření, provádí se interní audity a sestavuje se zpráva o stavu ISMS, na jejímž základě se bude ISMS přehodnocovat. [3]

Udržování a zlepšování ISMS (jednej)

Dochází ke sběru podnětů ke zlepšení ISMS a k nápravě tzv. neshod, které vyplývají z přezkoumání systému řízení ze strany vedení organizace v předchozí etapě. Zavádí se také nápravná nebo preventivní opatření po odstranění nedostatků. V této etapě je dosahováno tzv. neustálého zlepšování ISMS. [3]



Obrázek 3: Model PDCA v ISMS (Převzato z [4])

Koncept modelu PDCA poskytuje schématické vyjádření životního cyklu celého integrovaného systému řízení nebo jeho komponent a zároveň zajišťuje i tzv. zpětnou

vazbu. Součástí modelu PDCA je dokumentace každé jeho etapy (činnosti), která je nutná pro následnou optimalizaci jednotlivých procesů. [3] [4]

Více informací o jednotlivých etapách zavádění ISMS se dozvíte v kap. 2.7.1.

2.4 Řízení informačních technologií a bezpečnosti informací

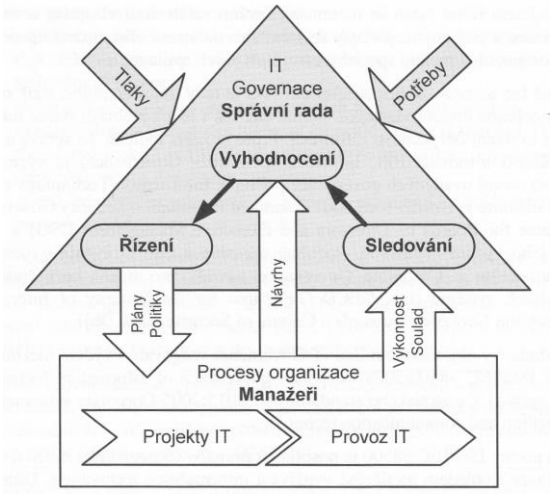
2.4.1 Koncepce řízení

V současné době se nejvíce používají dvě koncepce řízení informačních technologií v organizaci – **IT Governance** a **IT Service Management**. První z nich vznikla logickým rozšířením koncepce Corporate Governance a Enterprise Governance. Druhá z nich se zaměřuje na nižší úroveň řízení a jejím cílem je poskytování služeb informačních technologií. [3]

2.4.1.1 IT Governance (ITG)

Zabývá se odpovědným řízením a také chováním vlastníků a vedení organizace ve vztahu k informačním technologiím. Vytváří základní rámec pro rozhodování, jehož cílem je zajistit propojení informačních technologií s kulturou a strategií organizace. Zabývá se rozhodovacími procesy (např. určováním směru vývoje, zaváděním standardů, stanovením priorit investic), ne jejich realizací (za ni odpovídá vedení organizace). [3]

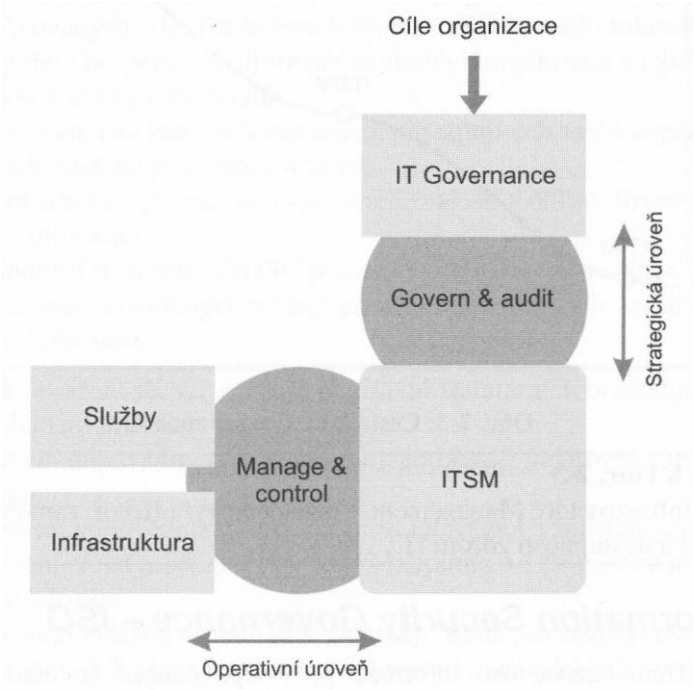
IT Governance lze definovat jako strukturu řídících vztahu a procesů umožňujících dosažení cílů organizace realizací přidané hodnoty za současného vyrovnání rizika s návratností investic do informačních technologií. [3]



Obrázek 4: Model ITG (Převzato z [3])

2.4.1.2 IT Service Management (ITSM)

IT Service Management je postup, který respektuje principy a praktiky pro návrh, dodávku a správu služeb IT v dohodnuté kvalitě, podporující klíčové aktivity zákazníka. [3]



Obrázek 5: Vztah ITG a ITSM (Převzato z [3])

Ačkoliv mají IT Governance a IT Service Management mnoho společného, lze mezi nimi najít zásadní rozdíly. Koncepce IT Governance nabízí širší pojetí orientované na strategická hlediska organizace a jejím hlavním cílem je definovat strategické cíle informačních technologií v souladu s potřebami a zájmy organizace, zatímco IT Service Management se zabývá taktickou a operativní úrovní s cílem účelně a účinně realizovat cíle stanovené řízením informačních technologií. [3]

2.4.2 Rámce a metodiky

Slouží jako podpora ve formě různých standardů, nejlepších praktik nebo metodik pro výše zmíněné koncepce řízení informačních technologií a bezpečnost informací v organizaci. V současné době se nejčastěji používají rámec ITIL a metodika COBIT, které jsou obecněji zaměřené a zabývají se kromě bezpečnosti informací také jinými aspekty řízení informačních technologií. [3]

2.4.2.1 Information Technology Infrastructure Library (ITIL)

ITIL je knihovna přístupů pro oblast řízení IT služeb a souvisejících procesů sloužící k zajištění dodávky kvalitních IT služeb za přiměřených nákladů. [3] [4]

Soustřeďuje se na plánování, vytváření, modifikaci, dodávku, správu, analýzu a použití služeb IT. Cílem rámce ITIL je poskytování uceleného souboru tzv. nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů. [3]

Nejedná se o normu, ani o metodiku, ale o rámec obsahující doporučení a osvědčené postupy, které vychází z již zmíněných nejlepších praktických zkušeností. [4]

Knihovna ITIL V3 (2007) je rozdělena do několika částí (knih) zaměřených na specifickou oblast řízení IT služeb [3] [4]:

- Strategie služeb (Service Strategy)
- Návrh služeb (Service Design)
- Implementace služeb (Service Transition)
- Provoz služeb (Service Operation)
- Průběžné zlepšování služeb (Continual Service Improvement)

Charakteristické znaky knihovny ITIL [3]:

- Procesní přístup
- Nejlepší praktické zkušenosti
- Respektování individuality
- Zákaznická orientace
- Jednotná terminologie
- Nezávislost na platformě

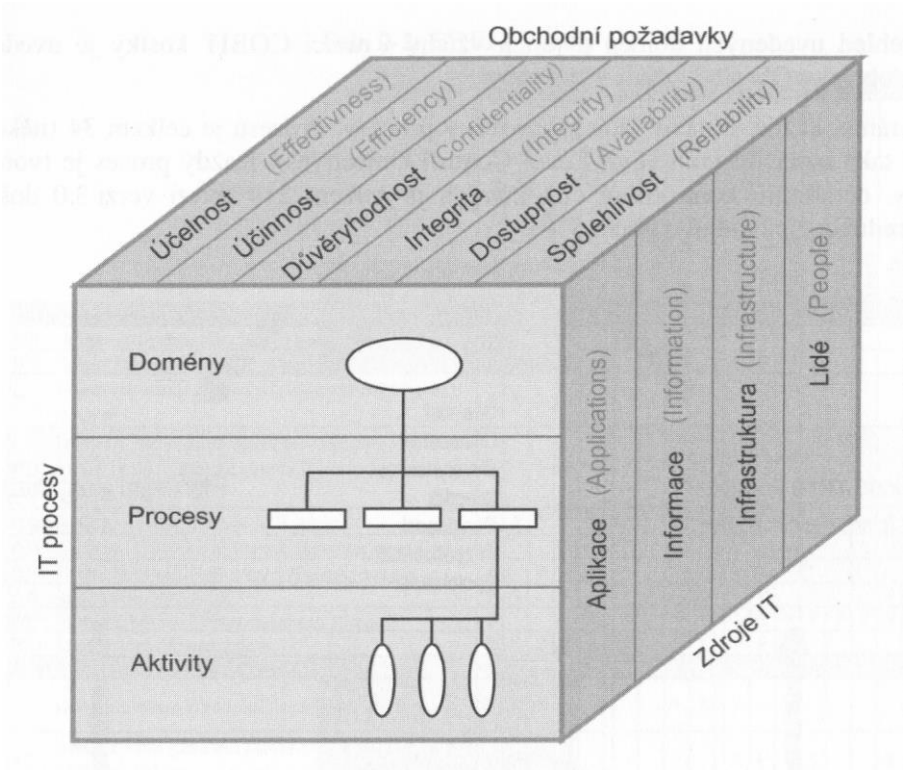
2.4.2.2 Control Objectives for Information and Related Technology (COBIT)

Metodika COBIT je sadou všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, jejímž cílem je maximalizace užitku plynoucího z informačních technologií v organizaci. [3]

Základní princip metodiky COBIT je na postaven na cílech organizace, zdrojích informačních technologií a procesech. Základní koncepcí tedy je, že zdroje informačních

technologií jsou řízeny procesy tak, aby bylo dosaženo stanovených cílů informačních technologií, které odpovídají strategickým požadavkům organizace. [3]

Základní koncepci metodiky COBIT vystihuje tzv. COBIT kostka:



Obrázek 6: COBIT kostka (Převzato z [3])

Z provedených studií vyplývá, že metodika COBIT je komplexnější než rámec ITIL, ten ovšem detailněji řeší některé oblasti. Obecně lze říct, že s každou novou verzí těchto dvou prostředků k řízení informačních technologií dochází k jejich vzájemnému sbližování. V této souvislosti je ale ovšem nutné konstatovat, že každý z nich si ponechává svoje specifika vyplývající z účelu, za kterým byly navrženy. Doporučením expertů je vhodně kombinovat oba způsoby řízení pro splnění požadavků konkrétního prostředí. [3]

2.5 Normalizační instituce

ISO – International Organization for Standardization

Posláním ISO je podpora rozvoje celosvětových standardizačních a aktivit s tím spojených se zaměřením na usnadnění mezinárodních směn zboží, služeb a na spolupráci ve sféře intelektuálních, vědeckých, technologických a ekonomických aktivit. [4]

IEC – International Electrotechnical Commision

IEC je celosvětová organizace, která připravuje a vydává mezinárodní normy z oblasti elektrotechnických, elektronických a jim příbuzných odvětví (elektřina, magnetismus, elektromagnetismus, elektroakustika, multimédia, telekomunikace, výroba a distribuce energií, terminologie, měření, navrhování a také bezpečnost). [4]

ITU – International Telecommunications Union

ITU je mezinárodní organizaci spadající do hierarchie OSN. Normalizační aktivity ITU, které již podpořily růst nových technologií jako např. mobilní technologie a internet, se nyní věnuje stavebním prvkům objevujícím se v globální informační infrastruktuře a k tvorbě vyspělých multimediálních systémů, které využívají slučování hlasových, datových, zvukových a video signálů. ITU zastává vedoucí roli ve správě spekter radiových frekvencí a tím zaručuje, že radiově založené systémy (např. mobilní telefony, letecké a námořní naváděcí systémy, satelitní komunikace, radiové a televizní vysílání atd.) mohou dál poskytovat spolehlivé bezdrátové služby. [4]

ČSNI – Český normalizační institut

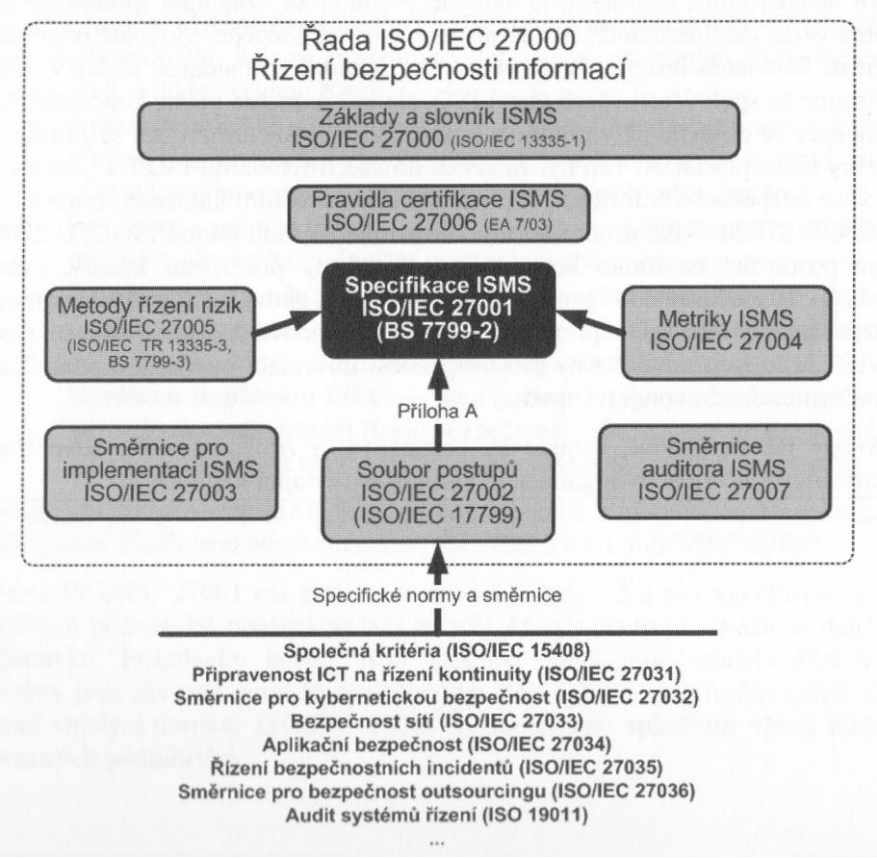
Český normalizační institut (ČSNI) byl zřízen jako státní příspěvková organizace a v současné době patří mezi organizace podřízené Ministerstvu průmyslu a obchodu. ČSNI má statut národní normalizační organizace zastupující národní zájmy v mezinárodních a evropských normalizačních organizacích. ČSNI je členem mezinárodních normalizačních organizací ISO a IEC, evropských normalizačních organizací CEN a CENELEC a zastává funkci národní normalizační organizace v evropském normalizačním institutu pro telekomunikaci ETSI.

ČSN (česká technická norma) vzniká dvěma způsoby:

- přejímáním evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN ISO, ČSN IEC atd.),
- tvorbou původních ČSN vyplývajících z národních potřeb a z hledisek zachování funkčnosti fondu ČSN. [4]

2.6 Normy

Řada norem pro řízení bezpečnosti informací ISO/IEC 27000 vychází z konceptu PDCA a její základem jsou normy, které jsou uvedeny na obrázku níže. Důležitou skutečností pro úspěšný rozvoj série ISO/IEC 27000 je vyjasnění vztahu s ostatními bezpečnostními normami. Velká pozornost je věnována tomu, aby bezpečnostní opatření byla navázána na normy, které hlouběji rozebírají určité oblasti bezpečnosti. Podobně jako u jiných systémů řízení je za jádro normalizace považována definice systému, v případě řízení bezpečnosti informací se tak klíčovým prvkem stává mezinárodní norma ISO/IEC 27001. [3]



Obrázek 7: Řada norem ISO/IEC 27000 (Převzato z [3])

V následující části se zabývám normami, které jsem při tvorbě této práce nejvíce využíval.

ČSN ISO/IEC 27000

Norma poskytuje přehled systémů řízení bezpečnosti informací, které tvoří předmět řady norem ISMS a definuje související termíny. Rodina norem má pomoci organizacím všech typů a velikostí zavést a provozovat systém ISMS. [4]

Úkolem této normy je sjednotit odborný slovník a definovat základní modely uplatňované při řízení bezpečnosti informací. [3]

ČSN ISO/IEC 27001

Norma poskytuje doporučení, jak aplikovat vybraná opatření z normy ISO/IEC 27002 v rámci procesu ustanovení, provozu, údržby a zlepšování systému řízení bezpečnosti informací v organizaci. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí model PDCA, který může být aplikován na všechny procesy ISMS tak, jak jsou definovány touto normou. [4]

V hlavní části normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumávání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému řízení bezpečnosti informací. Jsou zde specifikovány požadavky na výběr a zavedení bezpečnostních opatření chránících aktiva. [4]

Poskytuje normativní požadavky na vývoj a provoz ISMS, včetně sady opatření pro řízení a zmírnění rizik spojených s informačními aktivy, které se organizace provozováním ISMS snaží chránit. Organizace provozující ISMS mohou mít příslušnou shodu doloženou auditem a certifikací. Cíle opatření a opatření z přílohy A ISO/IEC 27001 musí být vybrány jako součást procesu ISMS na pokrytí identifikovaných požadavků. Cíle opatření a opatření uvedené v příloze A ISO/IEC 27001 jsou přímo odvozené z cílů opatření a opatření uvedených v ISO/IEC 27002. [2]

ČSN ISO/IEC 27002

Norma ISO/IEC 27002 obsahuje 114 bezpečnostních opatření rozdělených do 14 oblastí, viz kap. 2.10. Norma obsahuje podrobný výklad bezpečnostních opatření, která lze použít pro dosažení cílů, které jsou u jednotlivých kategorií opatření stanoveny. Norma nepřikazuje, která opatření musí být aplikována, ale ponechává rozhodnutí na organizaci.

Vhodnost implementace jednotlivých opatření je stanovena na základě analýzy rizik a jejich aplikace je závislá na konkrétní situaci v organizaci. Cílem není implementovat všechna bezpečnostní opatření, která norma popisuje, ale naplnit všechny aplikovatelné cíle opatření. Tento přístup zajišťuje širokou použitelnost normy a určitou flexibilitu při její implementaci. [4]

ČSN ISO/IEC 27005

Norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace. Definuje pravidla a postupy řízení rizik, ale neurčuje konkrétní metodiku pro řízení rizik bezpečnosti informací, což znamená, že je kompatibilní s již existujícími metodami pro řízení rizik. Norma je aplikovatelná na všechny typy organizací, které chtějí řídit rizika bezpečnosti informací – záleží tedy jen na organizaci, jaký přístup pro řízení rizik zvolí (např. v závislosti na rozsahu ISMS, kontextu řízení rizik, odvětví atd.). [4]

Poskytuje návod pro implementaci procesně orientovaného přístupu k řízení rizik, aby tak pomohla uspokojivě implementovat a splnit požadavky na řízení rizik bezpečnosti informací uvedené v ISO/IEC 27001. [2]

2.7 Systém řízení bezpečnosti informací (ISMS)

Systém řízení bezpečnosti informací (ISMS) sestává z politik, postupů, směrnic a příslušných zdroj a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Je založen na posuzování rizik a na úrovních přijetí rizik organizace, které byly navrženy pro efektivní ošetření rizik a pro jejich řízení. [2]

Zavedení ISMS by mělo být pro organizaci strategické rozhodnutí, a je nutné, aby toto rozhodnutí bylo uceleně začleněno, odstupňováno a aktualizováno v souladu s potřebami organizace. Zavedením řady norem ISMS mohou organizace demonstrovat obchodním partnerům a dalším zainteresovaným stranám svoji schopnost používat konzistentní a vzájemně uznávané principy bezpečnosti informací. [2]

Úspěšné zavedení ISMS pro ochranu informačních aktiv organizaci umožňuje:

- dosáhnout větší záruky, že její informační aktiva jsou neustále adekvátně chráněna před hrozbami,

- udržovat strukturovaný a komplexní rámec pro:
    - identifikování a posuzování rizik bezpečnosti informací,
    - výběr a implementaci použitelných opatření,
    - měření a zvyšování efektivnosti implementovaných opatření,
- neustále zlepšovat prostředí, ve kterém se řízení bezpečnosti informací uskutečňuje,
- efektivně docílit souladu s právními normami a předpisy. [2]

2.7.1 Etapy zavádění ISMS

Systém řízení bezpečnosti informací je založen na modelu PDCA. V kap. 2.3 je stručně popsán obsah a cíle jednotlivých etap navázaných na čtyři základní činnosti modelu PDCA. Použití modelu v ISMS je zachyceno na obrázku ve výše zmíněné kapitole. V následujícím textu více přiblížím obsah jednotlivých etap.

2.7.1.1 Ustanovení ISMS

Etapu lze rozdělit do následujících skupin činností:

- definice rozsahu, hranic a vazeb ISMS,
- definice a odsouhlasení prohlášení o politice ISMS,
- analýza a zvládání rizik,
    - definice přístupu organizace k hodnocení rizik,
    - identifikace rizika včetně určení aktiv a jejich vlastníků,
    - analýza a vyhodnocení rizik,
    - identifikace a ohodnocení variant pro zvládání rizik,
    - výběr cílů opatření a jednotlivých opatření pro zvládání rizik,
- souhlas vedení organizace s navrhovanými zbytkovými riziky a zavedením ISMS,
- příprava prohlášení o aplikovatelnosti. [3]

Prohlášení o politice ISMS

Rozsahově krátký, ale významově důležitý dokument, který vyjadřuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základem pro celý ISMS. [3]

Vzniká na základě specifických potřeb organizace a z praktického hlediska je důležité, aby politika ISMS:

- upřesnila cíle ISMS a definovala základní směr a rámec pro řízení bezpečnosti informací,
- zohlednila cíle a požadavky organizace a související zákonné, regulační a smluvní požadavky,
- vytvořila potřebné vazby po vybudování a údržbu ISMS v dané organizaci,
- stanovila kritéria, podle kterých jsou identifikována a hodnocena rizika,
- byla schválena vedením organizace. [3]

Prohlášení o aplikovatelnosti

V praxi nejdůležitější dokument, který postihuje systémové vazby ISMS. Nejčastěji zobrazuje matici vztahů mezi zjištěnými riziky a vybranými bezpečnostními opatřeními, z níž jsou pak jasné důvody pro nasazení jednotlivých opatření. Prohlášení o aplikovatelnosti představuje i formu zpětné vazby, protože podle něj lze jednoduše zkontrolovat, zda zavedením vybraných opatření došlo k pokrytí identifikovaných rizik. [3]

2.7.1.2 Zavádění a provozování ISMS

Etapa se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena v předchozí etapě.

Během této etapy je nutné provést následující činnosti:

- formulovat plán zvládání rizik a začít s jeho zaváděním,
- zavést navržená bezpečnostních opatření,
- vytvořit příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací,
- definovat program budování bezpečnostního povědomí a provést přípravu školení uživatelů, manažerů a dalším odborných pracovníků zejména z oblasti řízení bezpečnosti,
- upřesnit způsoby měření činnosti bezpečnostních opatření a sledovat stanovené ukazatele,

- zavést postupy a další opatření pro rychlou detekci bezpečnostních incidentů a reakci na ně,
- řídit zdroje, dokumenty a záznamy ISMS. [3]

2.7.1.3 Monitorování a přezkoumávání ISMS

Cílem etapy je zajistit účinné zpětné vazby. Mělo by tedy dojít k prověření všech zavedených bezpečnostních opatření a jejich dopadů na ISMS. Důležitým faktorem je nezávislé posouzení fungování a účinnosti ISMS pomocí interních auditů ISMS. Obecným cílem všech použitých zpětných vazeb je připravit dostatek podkladů o skutečném fungování ISMS, které budou předloženy vedení za účelem přezkoumání, zda je realizace ISMS v souladu s obecnými potřebami organizace. [3]

Během této etapy je třeba provést následující činnosti:

- monitorovat a ověřovat účinnost prosazení bezpečnostních opatření,
- provést audity ISMS, jejichž náplň pokryje celý rozsah ISMS,
- připravit zpráv o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni organizace včetně revize zbytkových a akceptovaných rizik. [3]

2.7.1.4 Udržování a zlepšování ISMS

V této fázi by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků (tzv. neshod), které se v ISMS vyskytují.

Během této etapy je nutné provést následující činnosti:

- zavádět identifikované možnosti zlepšení ISMS (především na základě přehodnocení vedením),
- provádět odpovídající opatření k nápravě nedostatků,
- implementovat preventivní opatření pro odstranění nedostatků. [3]

2.7.2 Povinná dokumentace

Dokumentace musí obsahovat záznamy o rozhodnutích učiněných vedením organizace. Veškeré činností musí být zpětně identifikovatelné v politikách a dohledatelné v záznamech, aby se zajistila jejich opakovatelnost. [4]

Seznam dokumentů, které ISMS vyžaduje [4]:

- Rozsah a hranice ISMS;
- Politika ISMS;
- Definice a popis přístupu k hodnocení rizik;
- Identifikace a ohodnocení aktiv;
- Identifikace rizik;
- Analýza rizik;
- Návrh opatření;
- Cíle opatření a bezpečnostní opatření pro zvládání rizik;
- Akceptace rizik;
- Získání povolení k provozování ISMS v rámci organizace;
- Prohlášení o aplikovatelnosti.

2.7.3 Budování bezpečnostního povědomí

Budování bezpečnostního povědomí je stejně jako informační bezpečnost nekončící proces. Není závislé na zavedení bezpečnostních opatřeních a systému řízení informační bezpečnosti, může tedy být (a mělo by být) prováděno zcela nezávisle. [7]

Na budování bezpečnostního povědomí lze nahlížet třemi způsoby, a to z hlediska:

- úrovní vzdělávání (povědomí, školení, vzdělávání, profesní rozvoj a certifikace),
- skupin uživatelů (začátečník, středně pokročilý, pokročilý),
- funkčního dělení a dělení dle vazeb na ICT. [7]

2.7.3.1 Plán zavedení

1. Určení rolí a odpovědností
2. Stanovení cílů pro každou úroveň vzdělávání
3. Rozdělení uživatelů do skupin dle znalostí
4. Určení cílů a vytvoření školících materiálů pro každou skupinu
5. Určení problematiky, která se bude v jednotlivých kurzech řešit
6. Metodiky, které budou při budování vzdělávacího programu použity
7. Dokumentace průběhu výuky a zpětné vazby
8. Vyhodnocení zpětné vazby a aktualizace výukových materiálů

9. Určení četnosti opakování vzdělávání a aktualizace výukových materiálů
10. Zhodnocení výsledků vzdělávání

Konkrétní plán zavedení budování bezpečnostního povědomí naleznete v kap. 4.4.2, která se zabývá návrhem opatření pro bezpečnost lidských zdrojů.

2.7.3.2 Způsoby řízení bezpečnostních školení

- **Centralizovaný** – veškerá odpovědnost na odpovědné osobě (např. CISO).
- **Částečně decentralizovaný** – politiky a školící strategie na odpovědné osobě, delegace implementačních a operativních povinností na jiné osoby.
- **Plně decentralizovaný** – vytvoření politiky na odpovědné osobě, delegace ostatních činností na jiné osoby.

2.7.3.3 Srovnávací rámec bezpečnostního vzdělávání

Tabulka 1: Srovnávací rámec bezpečnostního vzdělávání (Upraveno dle [7])

	Povědomí	**Školení**	**Vzdělání**
Vlastnost	„co“	„jak“	„proč“
Úroveň	informativní	znalostní	odborná
Cílová skupina uživatelů	záčátečník, středně pokročilý, pokročilý	středně pokročilý, pokročilý	pokročilý
Cíl	rozpoznání, zapamatování	dovednost	porozumění
Příklad výukových prostředků	výuková videa, prospekty, brožury	výukové materiály, případové studie, praktické ukázky	diskuze, semináře, studium
Způsob prokázání získaného vzdělání	uzavřené otázky typu "pravda/nepravda"	řešení problémů (praktická cvičení)	esej
Časová náročnost	krátkodobá	střednědobá	dlouhodobá

2.7.3.4 Certifikace

Potvrzení či doložení znalostí je možné např. pomocí certifikací, které nabízí mezinárodní organizace ISACA (Information Systems Audit and Control Association) sdružující profesionály z oblasti informačních technologií se zaměřením na oblast auditu, řízení, kontroly a bezpečnosti informačních systémů.

Příklad nabízených certifikací:

CISM (Certified Information Security Manager) – určena manažerům informační bezpečnosti a osobám odpovědným za řízení informační bezpečnosti.

CISA (Certified Information Systems Auditor) – určena auditorům a osobám zodpovědným za provádění kontrol v oblasti řízení informační bezpečnosti.

2.8 Aktiva

V kap. 2.1 jsem aktivum definoval jako hmotný nebo nehmotný majetek, který má pro organizaci nějakou hodnotu. Hodnota aktiva se určuje pomocí zvolené stupnice a hodnotících kritérií. Stupnice může vyjadřovat hodnotu aktiva v peněžních prostředcích, nebo kvalitativní hodnotu aktiva pro společnost vyjádřenou výrazy jako např. od „nedůležité“ až po „existenčně důležité“. Nejjednodušším a také nejpoužívanějším způsobem určení hodnoty aktiva je tzv. součtový algoritmus, kde se hodnota aktiva určí na základě dostupnosti, důvěrnosti a integrity (více v kap. 4.2.1). [4]

2.9 Rizika

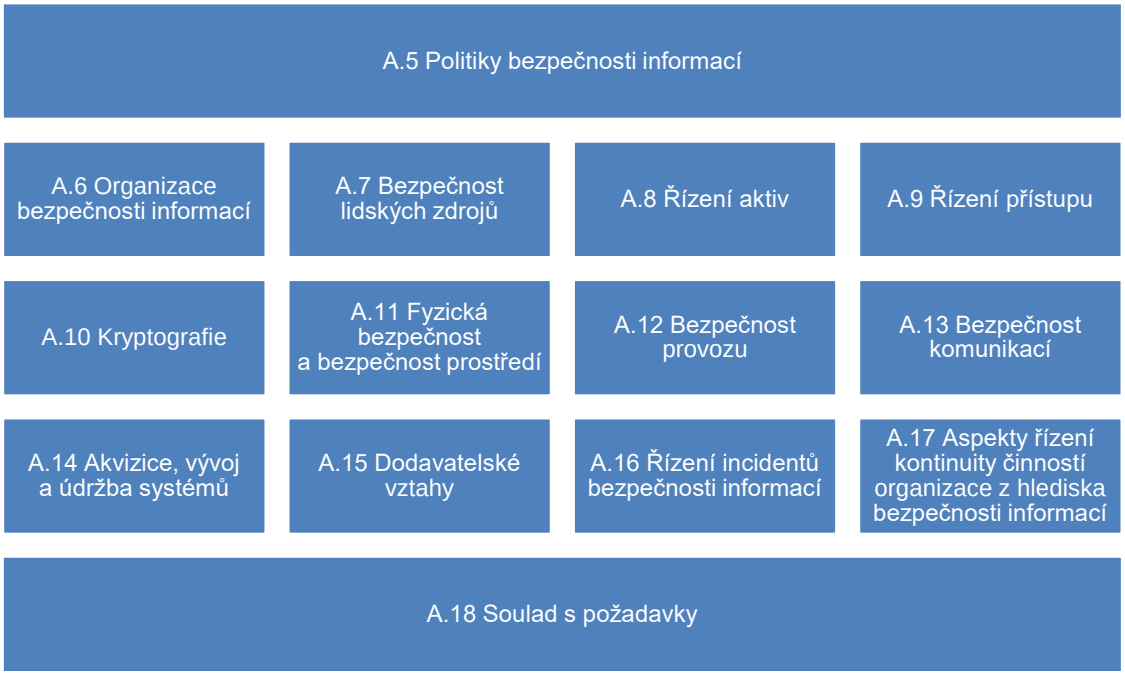
V kap. 2.1 jsem riziko definoval jako pravděpodobnost ohrožení aktiva, které vzniká kombinací hrozby a zranitelnosti aktiva. Míru (hodnotu) rizika lze určit pomocí dvou kvalitativních metod – buď se dvěma, nebo třemi parametry. Metoda se dvěma parametry definuje míru rizika pomocí pravděpodobnosti a dopadu incidentu. Metoda se třemi parametry určuje míru rizika pomocí pravděpodobnosti výskytu hrozby, hodnoty aktiva a zranitelnosti daného aktiva. [4]

V praktické části jsem použil metodu se třemi parametry (více v kap. 4.2.3).

2.10 Opatření

Principem, resp. cílem zavedení opatření je zvládání případných rizik. Problematika výběru opatření je popsána v normě ISO/IEC 27002. [4]

Norma ISO/IEC 27002:2014 obsahuje 114 bezpečnostních opatření rozdělených do následujících 14 oblastí:



Obrázek 8: Oblasti ISMS dle přílohy A normy ISO/IEC 27002 (Upraveno dle [8])

Výběrem, resp. návrhem jednotlivých opatření po zvládání rizik se zabývá kap. 4.4.

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Představení společnosti

Společnost se zabývá vývojem softwarových nástrojů a také optimalizací metodik pro podporu servisních procesů. Hlavními produkty společnosti jsou informační systémy pro řízení služeb a zdrojů především v odděleních správy informačních a komunikačních technologií. Společnost má dvě pobočky a zaměstnává zhruba 30 pracovníků. V jedné pobočce je realizován vývoj produktů, druhá pobočka je zaměřena především na poskytování služeb zákazníkům.

Vzhledem k podstatě a zaměření této práce si vedení společnosti nepřeje, aby byl v práci uveden její název a jakékoliv informace, které by mohly společnost potenciálně poškodit. V práci tedy nebudu uvádět citlivé informace, případně je vhodně upravím, aby podle nich společnost nebylo možné identifikovat, nebo využít informací spojených s její bezpečností.

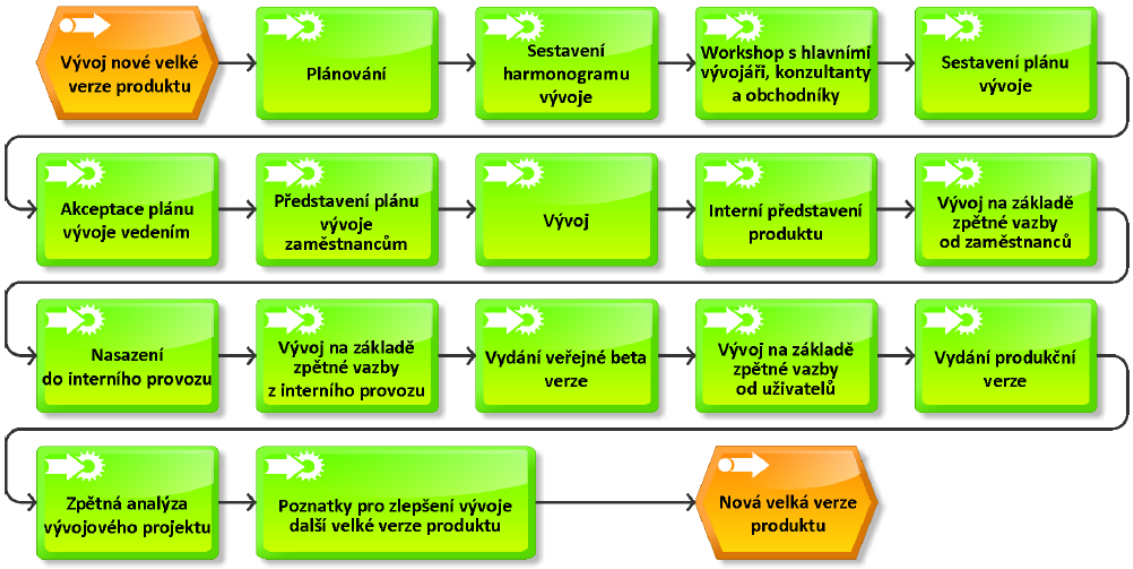
3.2 Podnikové procesy

V této práci se budu zabývat hlavními procesy, což jsou ty, které jsou předmětem podnikání společnosti, spotřebovávají největší část podnikových zdrojů, vytvářejí hodnotu pro zákazníky a vznikají z nich společnosti největší tržby. [6]

V případě vybrané společnosti lze za hlavní procesy považovat procesy vývoje produktů, jejich implementace u zákazníků a procesy vedoucí k získání, nebo udržení zákazníka, což jsou procesy prodeje a proces technické podpory.

Cílem této kapitoly není sestavit detailní analýzu podnikových procesů, ale pouze nastínit charakteristické podnikové procesy, z nichž budu při analýze rizik a návrhu bezpečnostních opatření vycházet. Podnikové procesy jsem navrhl na základě vlastní znalosti společnosti, komunikace se zaměstnanci, resp. vedením společnosti nebo z dostupných interních materiálů společnosti. Podnikové procesy jsem znázornil v programu Aris Express vždy jako jeden typický průběh daným procesem.

Vývoj velké verze produktu

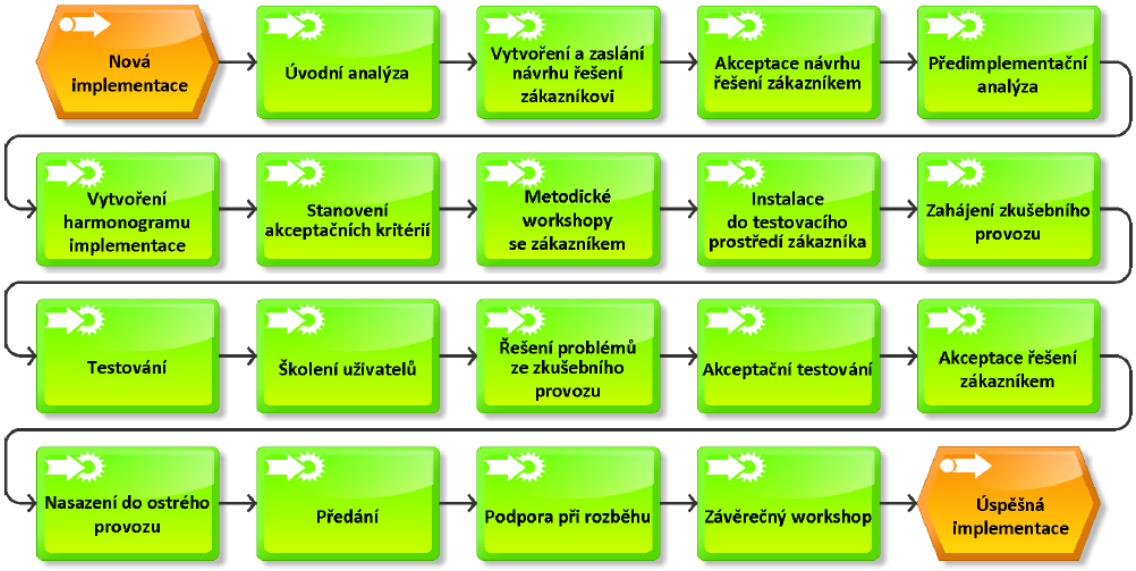


Obrázek 9: Proces vývoje velké verze produktu (Zdroj: vlastní zpracování)

Prodej

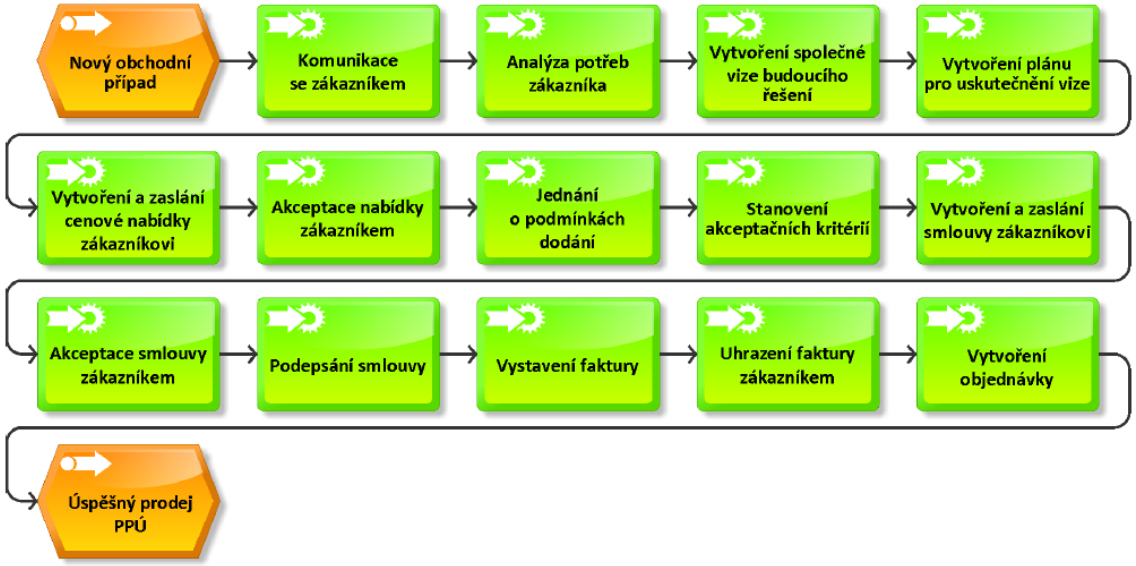
Obrázek 10: Proces prodeje (Zdroj: vlastní zpracování)

Implementace



Obrázek 11: Proces implementace (Zdroj: vlastní zpracování)

Prodej PPÚ (placené programové úpravy)

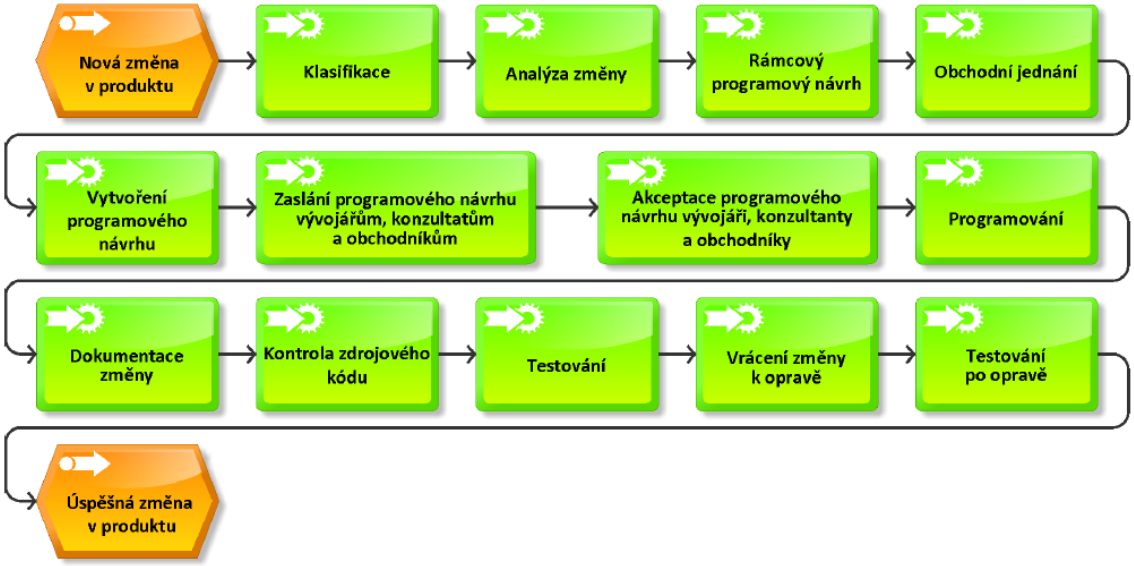


Obrázek 12: Proces prodeje PPÚ (Zdroj: vlastní zpracování)

Technická podpora (incident)

Obrázek 13: Proces technické podpory (Zdroj: vlastní zpracování)

Změna v produktu



Obrázek 14: Proces změny v produktu (Zdroj: vlastní zpracování)

Prodej (obnova) maintenance

Obrázek 15: Proces prodeje (obnovy) maintenance (Zdroj: vlastní zpracování)

Prodej (navýšení) licence

Obrázek 16: Proces prodeje (navýšení) licence (Zdroj: vlastní zpracování)

3.3 Současný stav bezpečnosti

V této práci beru při analýze a návrhu bezpečnostních opatření v úvahu pouze jednu ze dvou poboček společnosti. Bezpečnostní opatření mohou být pro druhou pobočku navržena a zavedena obdobným způsobem, resp. na základě úspěšné implementace v první pobočce. Používám-li tedy v textu výraz společnost (např. v souvislosti s již zmíněnou analýzou současného stavu, analýzou rizik nebo návrhem bezpečnostních opatření), myslím tímto výrazem pouze jednu pobočku společnosti.

V prostředí společnosti se používají počítače na platformě společnosti Microsoft a technologie Hyper-V, která platformu společnosti Microsoft zachovává. Jedná se tedy o unifikované řešení. Jiné operační systémy se v prostředí společnosti nepoužívají, nebezpečí napadení jiných operačních systémů tedy nehrozí.

Informační systémy, které společnost vyvíjí, společnost také používá v interním provozu. Informační systémy jsou vyvíjeny pro jednotnou platformu Microsoft a představují komplexní řešení (nemají návaznost na informační systémy nebo aplikace třetích stran).

3.3.1 Bezpečnostní politika a organizace bezpečnosti informací

Ve společnosti platí vnitřní směrnice, která stanovuje pravidla pro používání informačních technologií v prostředí společnosti jako např. pravidla pro uživatelské účty, software nebo ukládání dat.

Společnost má dále zavedenou směrnici týkající se bezpečnosti informací, která se zabývá také ochranou důvěrných informací, obchodních tajemství nebo osobních údajů. Určuje postupy, jak s informacemi nakládat, a povinnosti zaměstnanců při práci s nimi. Definuje také důsledky porušení bezpečnosti informací, povinnosti pro jednotlivá oddělení, bezpečnostní role a také určuje, jakým způsobem bude bezpečnost informací vynucována.

3.3.2 Řízení aktiv

Evidence a vlastnictví majetku (resp. aktiv) jsou řešeny v interním systému pro správu majetku. U majetku v evidenci je uveden vlastník nebo osoba, která za majetek odpovídá, nebo je majetek alespoň logicky přiřazen objektu (pobočka, oddělení, místnost), pod který patří, nebo ve kterém se fyzicky nachází.

3.3.3 Bezpečnost lidských zdrojů a řízení přístupu

Stávající zaměstnanci jsou pravidelně proškolováni v oblasti bezpečnosti informací, bezpečnosti a ochrany zdraví při práci a také v oblasti požární ochrany.

Každý zaměstnanec má v adresářové službě Active Directory vytvořen účet s vhodným nastavením práv přístupu k podnikovým prostředkům, čímž je mu umožněn přístup pouze k firemním službám a prostředkům, které potřebuje k vykonávání své práce.

Nový zaměstnanec při vzniku pracovního poměru podepíše smlouvu, ve které je seznámen např. s povinností zachovávat obchodní tajemství a mlčenlivost. Po nástupu je zaměstnanec seznámen s pravidly pro používání informačních technologií, směrnicí o bezpečnosti informací, bezpečností a ochranou zdraví při práci a také s požární ochranou. Při ukončení pracovního poměru zaměstnanec podepisuje smlouvu, která mimo jiné upřesňuje povinnost zachovávat obchodní tajemství, mlčenlivost a další náležitosti, kterými se společnost právně chrání. Odcházející zaměstnanci se musí před svým odchodem postarat o trvalé smazání podnikových dat ze všech zařízení a vrátit veškerý svěřený nebo zapůjčený majetek. Správce informačních technologií se poté postará o přesměrování e-mailu na jiného zaměstnance a zablokování účtu odcházejícího zaměstnance ve službě Active Directory, čímž je odcházejícímu zaměstnanci znemožněn přístup k firemním službám a prostředkům. Příchod i odchod zaměstnanců je procesně řešen pomocí interního systému pro řízení požadavků a služeb.

Směrnice týkající se uživatelských účtů (hesla, karty a certifikáty):

- Každý uživatel má svůj unikátní uživatelský účet (jméno a heslo, přístupovou kartu, certifikáty apod.), pomocí kterého ověřuje svoji identitu v systémech IT.
- Uživatel nesmí prozradit jiné osobě svoje heslo (ani nadřízenému, ani lidem z IT).
- V případě zjištění, že je heslo vyzrazeno nebo ztracena karta, musí zaměstnanec zajistit změnu hesla nebo přístupové karty, nebo celého uživatelského účtu.
- V případě zneužití uživatelského účtu nese veškerou odpovědnost zaměstnanec, kterému byl účet vytvořen.
- Při odchodu od počítače je uživatel povinen zamknout počítač (např. spořičem obrazovky s heslem, kombinací kláves Windows + L). Doporučuje se uložit všechny otevřené soubory.

3.3.4 Fyzická bezpečnost a bezpečnost prostředí

Kanceláře společnosti se nachází v druhém nadzemním poschodí bytového domu v prostorách dvou bytů, které jsou vzájemně propojené průchodem. Oba byty mají svůj vlastní vchod a je na zaměstnancích, který z nich použijí. Vchodové dveře do bytů a vstupní dveře do budovy jsou opatřeny zámky, od nichž má každý zaměstnanec klíče. Každý zaměstnanec má přístup do všech místností v rámci dané pobočky, včetně např. místnosti se servery a aktivními síťovými prvky. Servery jsou napájené přes zdroj nepřerušovaného napájení (UPS), který je v případě výpadku elektřiny vydrží napájet po dobu 30 minut. Komunikační a napájecí infrastruktura je vzájemně oddělena, k rušení tedy nedochází. Vodovodní rozvody jsou kromě kuchyňky, koupelny a sociálních zařízení také v jedné malé kancelářské místnosti, kde jsou ovšem zapečetěny – poškození zařízení způsobené vodou je tedy nepravděpodobné. Kancelářské prostory jsou klimatizovány. V místě průchodu z jednoho bytu do druhého je umístěn hasící přístroj.

3.3.5 Řízení komunikací a řízení provozu

Uživatelem (resp. správcem) v této kapitole je myšlen uživatel (resp. správce) informačních technologií v prostředí společnosti.

Pro používání software v prostředí společnosti platí:

- Uživatel nesmí používat software způsobem, který není v souladu s licenčními podmínkami pro daný typ software (např. instalovat nelegální software, kopírovat software nebo ho dále šířit či upravovat).
- Každý počítač má svého správce software, který je zodpovědný za legalitu software na počítači.
- Softwarové licence jsou evidovány v interním systému pro správu majetku.
- Software nainstalovaný na firemních počítačích je automaticky inventarizován nejméně jednou ročně.

Pro ukládání dat platí:

- Uživatel ukládá veškeré elektronické informace (data, soubory apod.), související s činností společnosti na servery (síťové disky, databáze apod.).
- Pokud jsou ve výjimečných případech uloženy informace jinam (např. lokálně na počítači), je uživatel povinen je umístit na server ihned jak jen to bude možné.
- Uživatel nesmí ukládat na firemní disky hudební soubory, videa, obrázky, software a jiné soubory, které porušují autorská práva nebo zákony ČR.
- Uživatel nesmí sdílet jakákoliv data bez souhlasu nadřízených.

Pro zajištění bezpečnosti jsou nastavena tato pravidla:

- Uživatel zodpovídá za bezpečnost svěřených IT zařízení včetně dat.
- Uživatel dodržuje pravidla pro práci s hesly (viz níže).
- Uživatel se chová zodpovědně a provádí činnosti tak, aby nevystavoval svěřené zařízení riziku zneužití nebo napadení (vyvaruje se pohybu v šedých zónách internetu a nebrání automatickým aktualizacím software).
- Správci zodpovídají za nainstalování potřebných aktualizací software (antivirový a antispamový software, firmware, aktualizace software apod.).

Pravidla pro práci s hesly určená pro uživatele:

- Své heslo pro přihlášení do počítače si zapamatujte (nikam ho nepište) a nesdělujte ho svým kolegům.
- Citlivé přístupové údaje nikdy neuchovávejte v papírové podobě (v poznámkovém bloku, lístky přilepené na monitoru počítače apod.).

- Citlivé přístupové údaje nikdy společně neposílejte po jednom komunikačním kanále, využijte raději dva komunikační kanály (přístupové jméno pošlete jedním komunikačním kanálem, přístupové heslo pak druhým).

Správce informačních technologií provádí:

- Monitorování aktivity sítě (lokálně i do internetu), tzn. i přístup na web nebo příjem a odesílání e-mailů.
- Skenování hardware a software na všech počítačích včetně sledování využití instalovaných aplikací.
- Sledování obsazenosti síťových disků.
- Vzdálené sledování pracovní plochy počítače uživatele (obvykle z důvodu okamžité pomoci při řešení problémů).
- Monitorování všech činností probíhající na serverech.

3.3.6 Zvládání bezpečnostních incidentů

Bezpečnostní incidenty se ve společnosti nahlašují pomocí interního systému řízení požadavků a služeb. V případě výskytu bezpečnostního incidentu uživatelé vytvoří nový požadavek ve službě určené pro hlášení podezření na ohrožení bezpečnosti informací a důvěrných dat. Nahlášený bezpečnostní incident poté začnou řešit pracovníci interního IT, kteří mohou s uživatelem, který bezpečnostní incident nahlásil, komunikovat (např. ho požádat o pomoc při bližší identifikaci problému). Po zvládnutí (vyřešení) bezpečnostního incidentu je žadatel informován e-mailem.

3.4 Zhodnocení současného stavu

Z analýzy je patrné, že ve společnosti již existují různé směrnice a pravidla, které definují např. používání uživatelských účtů, software, ukládání dat, zajištění obecné bezpečnosti v prostředí IT, práci s hesly a činnosti správce IT. Předpokládám, že bude potřeba vytvořit nové směrnice nebo upravit ty stávající tak, aby odpovídaly požadavkům jednotlivých opatření, které vyplynou z analýzy rizik.

Z analýzy současného stavu vyplývá, že bude potřeba např.:

- nastavit pravidla pro používání a zabezpečení mobilních zařízení, které se v již existujících směrnicích blíže neřeší,

- definovat a zajistit vzdělávání zaměstnanců v oblasti bezpečnosti informací,
- zavést řízení přístupu (správa oprávnění a jejich pravidelné přezkoumávání),
- zajistit kryptografická opatření, o kterých se směrnice nezmiňují,
- zajistit fungování podpůrných služeb (např. údržbu zdrojů nepřerušovaného napájení),
- zavést a řídit ochranu proti malware, zálohování a logování.

3.5 Očekávání a východiska vedení

Vedení společnosti od této práce očekává:

- analýzu současného stavu informační bezpečnosti,
- identifikaci a ohodnocení aktiv,
- analýzu rizik,
- návrh bezpečnostních opatření pro zvládání největších rizik,
- zvýšení bezpečnostního povědomí u zaměstnanců,
- zvýšení informační bezpečnosti ve společnosti.

Společnost se v současné době nechystá zavádět systém řízení informační bezpečnosti (ISMS). Vedení společnosti preferuje provedení expresní, nikoliv expertní, analýzy rizik.

3.6 Analýza konkurenčního prostředí

Pro získání většího přehledu o informační bezpečnosti v daném oboru podnikání jsem se rozhodl provést rychlou analýzu konkurentů společnosti z pohledu informační bezpečnosti. Z interních analýz konkurence jsem vybral několik konkurenčních společností, z jejichž webových stránek a dokumentů na nich dostupných jsem zjistil, že žádná z nich v současné době neposkytuje svým zákazníkům záruky v oblasti informační bezpečnosti. Žádný z analyzovaných konkurentů společnosti nemá zavedený systém řízení informační bezpečnosti (ISMS), stejně tak žádný z nich není certifikován dle ISO/IEC 27001. Na webových stránkách jedné vybrané konkurenční společnosti jsem našel informaci, že ačkoliv společnost nemá certifikaci dle ISO/IEC 27001, má zavedena některá bezpečnostní opatření dle normy ISO/IEC 27002, což by měl být také případ mnou analyzované společnosti po zavedení navržených opatření.

4 VLASTNÍ NÁVRH ŘEŠENÍ

Cílem této kapitoly je navrhnout vhodná bezpečnostní opatření na základě analýzy rizik a dostupných zdrojů společnosti dle norem řady ISO/IEC 27000. Normy řady ISO/IEC 27000 jsem se rozhodl použít proto, že se jedná o mezinárodní standard pro komplexní řízení informační bezpečnosti. V této kapitole jsem postupoval dle normy ISO/IEC 27001, protože podle této normy se provádí případná certifikace systému řízení informační bezpečnosti. Při návrhu bezpečnostních opatření jsem vycházel z normy ISO/IEC 27002.

4.1 Rozsah a hranice

Jelikož se společnost nechystá zavádět systém řízení informační bezpečnosti (ISMS), požadavkem a prioritou společnosti je zavedení bezpečnostních opatřeních pro zvládání největších rizik (těch s největším dopadem) na základě jejich analýzy a dostupných zdrojů podniku.

4.2 Analýza rizik

Nutným předpokladem pro analýzu rizik jsou identifikovaná a ohodnocená aktiva, kterých se případná rizika budou týkat. Analýza rizik tedy začíná identifikací a ohodnocením aktiv, pokračuje identifikací hrozeb a zranitelností a končí vyhodnocením rizik. Z výše jmenovaných parametrů (aktiva, hrozby, zranitelnosti) vyplývá, že jsem pro analýzu rizik použil maticovou metodu se třemi parametry.

Při analýze rizik jsem vycházel z analyzovaných podnikových procesů, komunikace s vedením podniku, vlastníky (garanty) a uživateli daných aktiv.

4.2.1 Identifikace a ohodnocení aktiv

Identifikoval jsem aktiva, která jsem poté ohodnotil na základě stupnice 1-5, kde nejméně důležité aktivum obdrží hodnotu „1“ a nejdůležitější aktivum obdrží hodnotu „5“.

Pro výpočet hodnoty aktiva jsem využil tzv. součtového algoritmu, který je nejjednodušším a nejpoužívanějším způsobem hodnocení aktiv, protože poskytuje nejrychlejší způsob získání hodnoty aktiva a také umožňuje zjištění dopadu, který bude poškození, příp. zničení daného aktiva pro organizaci mít [4]:

$$hodnota\ aktiva = \frac{(dostupnost + důvěrnost + integrita)}{3}$$

Tabulka 2: Hodnota aktiva (Zdroj: vlastní zpracování)

Hodnota aktiva	Dopad rizika (při napadení aktiva)	Míra rizika
1	žádný	bezvýznamná
2	zanedbatelný	akceptovatelná
3	potíže či finanční ztráty	nízká
4	vážné potíže či podstatné finanční ztráty	nežádoucí
5	existenční potíže	nepřijatelná

Tabulka 3: Ohodnocení aktiv (Zdroj: vlastní zpracování)

Aktivum (A)	Zdroj	Hodnota aktiva
Obchodní procesy a činnosti		
obchodní procesy a činnosti	servery, databázový systém (SQL)	5
Informace		
interní data	servery, databázový systém (SQL)	5
data zákazníků	servery, databázový systém (SQL)	4
zdrojové kódy	servery	4
zálohy	servery	5
Hardware		
servery	servery	5
klientské počítače	pracovní stanice, přenosné počítače	3
procesní periferie	tiskárny, telefony, přenosná úložiště	3
Software		
serverový operační systém	servery	4
databázový systém (SQL)	servery	4
informační systém	servery	5
klientský operační systém	pracovní stanice, přenosné počítače	2
Sítě		
síťová infrastruktura	síťové prvky, kabeláž	4
Služby		
elektrická energie	dodavatel elektrické energie	4
internetové připojení	poskytovatel internetového připojení	4
vzdálené připojení (VPN)	síťová infrastruktura, interní IT	4
servis, údržba, profylaxe	interní IT	2

Dílčí hodnoty dostupnosti, důvěrnosti a integrity pro jednotlivá aktiva naleznete v příloze.

4.2.2 Identifikace hrozeb a zranitelností

Identifikoval jsem hrozby, před kterými je třeba aktiva chránit, a pravděpodobnost, s kterou se hrozby mohou vyskytnout. Stejně jako u ohodnocení aktiv jsem použil stupnici 1-5, kde nejméně pravděpodobná hrozba obdrží hodnotu „1“ a nejvíce pravděpodobná hrozba obdrží hodnotu „5“.

Tabulka 4: Hodnota hrozby (Zdroj: vlastní zpracování)

Hodnota hrozby	Míra pravděpodobnosti výskytu
1	nahodilá
2	nepravděpodobná
3	pravděpodobná
4	velmi pravděpodobná
5	trvalá

Tabulka 5: Ohodnocení hrozeb (Zdroj: vlastní zpracování)

Hrozba (T)	Pravděpodobnost výskytu
Fyzické poškození	
Požár	2
Poškození vodou	2
Znečištění	3
Zničení zařízení nebo médií	2
Ztráta základních služeb	
Selhání klimatizace nebo dodávky vody	2
Přerušení dodávky elektřiny	3
Selhání internetového připojení	4
Ohrožení informací	
Vzdálená špionáž	2
Krádež médií nebo dokumentů	2
Krádež zařízení	2
Zprovoznění recyklovaných nebo vyřazených médií	1
Data pocházející z nedůvěryhodných zdrojů	3
Falšování pomocí technického vybavení	3
Falšování pomocí aplikačního progr. vybavení	3
Technická selhání	
Chybné fungování zařízení	3
Chybné fungování aplikačního progr. vybavení	3
Chyba údržby	2
Neoprávněné činnosti (vnitřní)	
Neoprávněné použití zařízení	2
Podvodné kopírování aplikačního progr. vybavení	2
Poškození dat	3
Nezákonné zpracování dat	1
Neoprávněné činnosti (vnější)	
Neoprávněné použití zařízení	2
Podvodné kopírování aplikačního progr. vybavení	3
Poškození dat	2
Nezákonné zpracování dat	2
Ohrožení funkčnosti	
Chyba v používání	2
Zneužití oprávnění	3

Z ohodnocených aktiv a hrozeb jsem sestavil matici zranitelností, která představuje zranitelnost daného aktiva vůči dané hrozbě.

Tabulka 6: Matice zranitelnosti (Zdroj: vlastní zpracování)

Zranitelnost (V)		**Aktivum**	obchodní procesy a činnosti	interní data	data zákazníků	zdrojové kódy	zálohy	servery	serverový operační systém	databázový systém (SQL)	informační systém	síťová infrastruktura	elektrická energie	internetové připojení	vzdálené připojení (VPN)
		A	5	5	4	4	5	5	4	4	5	4	4	4	4
Hrozba	**T**														
Požár	2						2	2				2	2	1	
Poškození vodou	2						2	2				2	3	2	
Znečištění	3							2				1			
Zničení zařízení nebo médií	2						2	1				1	2	2	
Selhání klimatizace nebo dodávky vody	2						1	2				1			
Přerušení dodávky elektřiny	3							5				3	5	5	
Selhání internetového připojení	4							3				2		5	4
Vzdálená špionáž	2		3	3	2	3	2		1	1	1				
Krádež médií nebo dokumentů	2		3	2	2	1	2			2	2				
Krádež zařízení	2											1	1	1	
Zprovoznění recyklovaných nebo vyřazených médií	1		3	2	1	2	3								
Data pocházející z nedůvěryhodných zdrojů	3									1	1				
Falšování pomocí technického vybavení	3							2				2		3	
Falšování pomocí aplikačního progr. vybavení	3								2	2	2			1	2
Chybné fungování zařízení	3							4				1	2	2	2
Chybné fungování aplikačního progr. vybavení	3								4	3	3	1		1	
Chyba údržby	2						2	2	3	1	1	2	1	1	
Neoprávněné použití zařízení	2		3	4	3	3	1	2				3		2	
Podvodné kopírování aplikačního progr. vybavení	2								2	2	1				
Poškození dat	3		2	4	3	4	5		2	4	3				
Nezákonné zpracování dat	1		4	5	4	3	4		1	5	4				
Neoprávněné použití zařízení	2		3	4	3	3	1	3				3			
Podvodné kopírování aplikačního progr. vybavení	3								2	2	1				
Poškození dat	2		2						2	2	1				
Nezákonné zpracování dat	2		4	4	3	4	5		2	4	3				
Chyba v používání	2			5	5	3	4	2	4	4	4	2	2	2	
Zneužití oprávnění	3		3	3	3	3	2	2	3	3	2	2		2	

Matici zranitelností v plném rozsahu naleznete v příloze.

4.2.3 Identifikace rizik

Využitím ohodnocených aktiv, hrozeb a zranitelností jsem sestavil matici rizik. Míru rizika jsem spočítal vztahem

$$R = T \times A \times V$$

kde R – míra rizika, T – pravděpodobnost hrozby, A – hodnota aktiva a V – zranitelnost aktiva.

Pro stanovení hraničních hodnot míry rizika jsem stejně jako u ohodnocení aktiv a hrozeb použil stupnici 1-5, kde nejméně významné riziko obdrží hodnotu „1“ a nejvíce významné riziko obdrží hodnotu „5“.

Tabulka 7: Hodnota rizika (Zdroj: vlastní zpracování)

Hodnota rizika	Míra rizika	Dopad
0-10	bezvýznamná	žádný
11-20	akceptovatelná	zanedbatelný
21-30	nízká	potíže nebo finanční ztráty
31-60	nežádoucí	vážné potíže nebo podstatné finanční ztráty
61 a více	nepřijatelná	existenční potíže

Tabulka 8: Matice rizik (Zdroj: vlastní zpracování)

Riziko (R)		**Aktivum**	obchodní procesy a činnosti	interní data	data zákazníků	zdrojové kódy	zálohy	servery	serverový operační systém	databázový systém (SQL)	informační systém	síťová infrastruktura	elektrická energie	internetové připojení	vzdálené připojení (VPN)
		A	5	5	4	4	5	5	4	4	5	4	4	4	4
Hrozba	**T**														
Požár	2						20	20				16	16	8	
Poškození vodou	2						20	20				16	24	16	
Znečištění	3							30				12			
Zničení zařízení nebo médií	2						20	10				8	16	16	
Selhání klimatizace nebo dodávky vody	2						10	20				8			
Přerušení dodávky elektřiny	3							75				36	60	60	
Selhání internetového připojení	4							60				32		80	64
Vzdálená špionáž	2		30	30	16	24	20		8	8	10				
Krádež médií nebo dokumentů	2		30	20	16	8	20			16	20				
Krádež zařízení	2											8	8	8	
Zprovoznění recyklovaných nebo vyřazených médií	1		15	10	4	8	15								
Data pocházející z nedůvěryhodných zdrojů	3									12	15				
Falšování pomocí technického vybavení	3							30				24		36	
Falšování pomocí aplikačního progr. vybavení	3								24	24	30			12	24
Chybné fungování zařízení	3							60				12	24	24	24
Chybné fungování aplikačního progr. vybavení	3								48	36	45	12		12	
Chyba údržby	2						20	20	24	8	10	16	8	8	
Neoprávněné použití zařízení	2		30	40	24	24	10	20				24		16	
Podvodné kopírování aplikačního progr. vybavení	2								16	16	10				
Poškození dat	3		30	60	36	48	75		24	48	45				
Nezákonné zpracování dat	1		20	25	16	12	20		4	20	20				
Neoprávněné použití zařízení	2		30	40	24	24	10	30				24			
Podvodné kopírování aplikačního progr. vybavení	3								24	24	15				
Poškození dat	2		20						16	16	10				
Nezákonné zpracování dat	2		40	40	24	32	50		16	32	30				
Chyba v používání	2			50	40	24	40	20	32	32	40	16	16	16	
Zneužití oprávnění	3		45	45	36	36	30	30	36	36	30	24		24	

Matici rizik v plném rozsahu naleznete v příloze.

4.2.4 Vyhodnocení analýzy rizik

Z matice rizik je patrné, že největší riziko představuje:

- ztráta základních služeb – přerušení dodávky elektřiny nebo selhání internetového připojení s největším dopadem na servery, síťovou infrastrukturu a služby,
- chybné fungování aplikačního programového vybavení s dopadem na software,
- neoprávněné činnosti v podobě poškození dat nebo jejich nezákonného zpracování se značným dopadem na interní data, zdrojové kódy a zálohy,
- chyba v používání nebo zneužití oprávnění, což může mít dopad na informační nebo softwarová aktiva.

To jsou největší rizika, kterými je potřeba se při návrhu opatření přednostně zabývat a navrhnout opatření pro jejich zvládání.

4.3 Akceptace rizik

Vedení společnosti rozhodlo, že budou akceptována rizika s bezvýznamnou, akceptovatelnou a nízkou mírou rizika (dále jen bezvýznamná, akceptovatelná a nízká rizika). Rizika s nežádoucí a nepřijatelnou mírou rizika (dále jen nežádoucí a nepřijatelná rizika) akceptována nebudou, navrhnu tedy bezpečnostní opatření pro jejich zvládání.

Tabulka 9: Akceptace rizik (Zdroj: vlastní zpracování)

Riziko (R)	Akceptace
Fyzické poškození	
Požár	ANO
Poškození vodou	ANO
Znečištění	ANO
Zničení zařízení nebo médií	ANO
Ztráta základních služeb	
Selhání klimatizace nebo dodávky vody	ANO
Přerušení dodávky elektřiny	NE
Selhání internetového připojení	NE
Ohrožení informací	
Vzdálená špionáž	ANO
Krádež médií nebo dokumentů	ANO
Krádež zařízení	ANO
Zprovoznění recyklovaných nebo vyřazených médií	ANO
Data pocházející z nedůvěryhodných zdrojů	ANO
Falšování pomocí technického vybavení	NE
Falšování pomocí aplikačního progr. vybavení	ANO
Technická selhání	
Chybné fungování zařízení	NE
Chybné fungování aplikačního progr. vybavení	NE
Chyba údržby	ANO
Neoprávněné činnosti (vnitřní)	
Neoprávněné použití zařízení	NE
Podvodné kopírování aplikačního progr. vybavení	ANO
Poškození dat	NE
Nezákonné zpracování dat	ANO
Neoprávněné činnosti (vnější)	
Neoprávněné použití zařízení	NE
Podvodné kopírování aplikačního progr. vybavení	ANO
Poškození dat	ANO
Nezákonné zpracování dat	NE
Ohrožení funkčnosti	
Chyba v používání	NE
Zneužití oprávnění	NE

4.4 Návrh opatření pro zvládání rizik

Soubor bezpečnostních opatření jsem převzal z normy ČSN ISO/IEC 27001:2014, přílohy A. Při návrhu bezpečnostních opatření jsem vycházel z normy ČSN ISO/IEC 27002:2014.

Vzhledem ke skutečnosti, že společnost se v současné době nechystá zavádět systém řízení informační bezpečnosti, nebudu navrhovat zavedení všech dostupných bezpečnostních opatření na základě analýzy rizik, ale pouze těch pro zvládání největších rizik a dostupných zdrojů podniku (např. finančních, časových nebo personálních). V této kapitole tedy navrhuji k zavedení opatření, která je potřeba zavést přednostně v první etapě zavádění, aby byla pokryta největší rizika.

Největšími riziky jsou chápána nežádoucí a nepřijatelná rizika, která znamenají vážné potíže nebo podstatné finanční ztráty, resp. existenční potíže pro organizaci a zároveň působí (mají dopad) na více než jedno aktivum.

Označení „ZAVÉST“ je v následující tabulce uvedeno u bezpečnostních opatření:

- pro zvládání největších rizik, která nejsou akceptována (nežádoucí a nepřijatelná rizika),
- která jsou již částečně zavedena, ale je potřeba je určitým způsobem modifikovat.

Označení „NEZAVÁDĚT“ bude uvedeno u bezpečnostních opatření:

- pro zvládání rizik, která jsou akceptována (bezvýznamná, akceptovatelná a nízká rizika),
- která jsou již zavedena a nepotřebují žádným způsobem modifikovat.

Tabulka 10: Opatření pro zvládání největších rizik (Zdroj: vlastní zpracování)

Hrozba (T)	Bezpečnostní opatření	Rozhodnutí
Ztráta základních služeb		
Přerušení dodávky elektřiny	A.11.2.2	ZAVÉST
Selhání internetového připojení	A.11.2.2, A.11.2.3	ZAVÉST
Technická selhání		
Chybné fungování aplikačního progr. vybavení	A.12.2.1, A.12.4.1	ZAVÉST
Neoprávněné činnosti (vnitřní)		
Poškození dat	A.9.2.3, A.9.4.1, A.11.2.8, A.12.2.1, A.12.3.1	ZAVÉST
Neoprávněné činnosti (vnější)		
Nezákonné zpracování dat	A.10.1.1, A.11.2.8, A.12.2.1, A.12.4.1	ZAVÉST
Ohrožení funkčnosti		
Chyba v používání	A.6.2.1, A.7.2.2, A.8.1.3, A.8.2.3, A.9.3.1, A.11.2.8, A.11.2.9	ZAVÉST
Zneužití oprávnění	A.7.2.3, A.9.2.3, A.9.2.5, A.9.4.1, A.12.4.1	ZAVÉST

Opatření navržená na základě analýzy rizik v plném rozsahu naleznete v příloze.

Opatření v příloze, která nejsou navržena k zavedení v první etapě, budou zavedena v dalších etapách.

K zavedení v první etapě jsem navrhl také opatření spadající do oblasti interní organizace bezpečnosti informací (A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4, A.6.1.5), která přímo nevyplývají z analýzy rizik, ale je vhodné je ve společnosti zavést z důvodu jejich obecné působnosti v oblasti informační bezpečnosti.

4.4.1 A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Všechny odpovědnosti za bezpečnost informací by měly být přiděleny a definovány.

Implementace: Identifikovat odpovědnosti za ochranu jednotlivých aktiv a za provádění specifických postupů v oblasti bezpečnosti informací. Definovat odpovědnosti

za činnosti v oblasti řízení rizik bezpečnosti informací, a zejména za přijetí zbytkového rizika. Identifikovat a definovat aktiva a procesy bezpečnosti informací. Každému aktivu přiřadit vlastníka, který za dané aktivum bude odpovědný. Umožnit pověřeným osobám udržovat krok s vývojem, aby byly schopné zastávat dané odpovědnosti.

Časová náročnost: 16 hodin

Náklady: Školení v oblasti řízení bezpečnosti informací – 15 000 Kč/osoba.

Poznámka: Předpokládám, že na školení v oblasti řízení bezpečnost informací bude vyslán pracovník, který odpovídá za bezpečnost informací v organizaci, a který bude dále poskytovat interní školení ostatním zaměstnancům.

A.6.1.2 Princip oddělení povinností

Opatření: Konfliktní povinnosti a oblasti působnosti by měly být odděleny, aby se omezily příležitosti pro neoprávněné nebo neúmyslné změny nebo zneužití aktiv organizace.

Implementace: Zajistit, aby žádná jednotlivá osoba nemohla k aktivům přistupovat, upravovat je nebo používat je bez oprávnění nebo detekce. Při návrhu opatření brát na vědomí možnost nekalých praktik. Je-li obtížné dostáhnout oddělení povinností (např. v malých organizacích), musí být zvážena další opatření jako je sledování činnosti, auditní záznamy a dohled managementu.

Doporučuji vytvořit např. dokument s popisem pracovních pozic, kde budou definovány role, práva, povinnosti, odpovědnosti osob, které tyto pracovní pozice zastávají. Dále je potřeba patřičné nastavení v Active Directory.

Časová náročnost: 4 hodiny

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Opatření: Měly by být udržovány přiměřené kontakty s příslušnými autoritami.

Implementace: Zavést postupy, které určují, kdy a kým by měly být kontaktovány autority (např. orgány vymáhající právo nebo orgány dohledu) a jak by měly být identifikované incidenty bezpečnosti informací včas hlášeny (např. existuje-li podezření, že došlo k porušení zákona).

Doporučuji např. odebírat novinky z webových stránek Národního centra kybernetické bezpečnosti (www.govcert.cz) nebo Národního CSIRT České republiky (www.csirt.cz). Vhodnou praktikou je zavádění preventivních opatření v organizaci např. na základě aktuálních hrozeb zmíněných v aktualitách na výše zmíněných webových stránkách.

Časová náročnost: 4 hodiny

A.6.1.4 Kontakt se zájmovými skupinami

Opatření: Měly by být udržovány přiměřené kontakty se zvláštními zájmovými skupinami nebo dalšími fóry specialistů na bezpečnost a profesními sdruženími.

Implementace: Zajistit členství ve zvláštních zájmových skupinách či fórech, která mohou sloužit jako prostředek např. k:

a) zlepšování znalostí o doporučených postupech a sledování aktuálního vývoje v příslušné oblasti bezpečnosti informací,
b) ujištění, že chápání bezpečnosti informací v organizaci je aktuální a kompletní,
c) obdržení včasných varování, doporučení a oprav týkajících se útoků a zranitelností,
d) získání přístupu k doporučením specialistů bezpečnosti informací,
e) sdílení a výměně informací o nových technologiích, produktech, hrozbách nebo zranitelnostech.

Časová náročnost: 2 hodiny

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Bezpečnost informací by měla být řešena v rámci řízení projektů, bez ohledu na typ projektu.

Implementace: Začlenit bezpečnost informací do metod řízení projektů v organizaci, aby byla identifikována rizika bezpečnosti informací a aby byla řešena jako součást projektu.

Používané metody řízení projektů by měly vyžadovat, aby:

a) cíle bezpečnosti informací byly zahrnuty do projektových cílů,
b) se posuzování rizik bezpečnosti informací provádělo již v rané fázi projektu, aby se následně identifikovala nezbytná opatření,
c) bezpečnost informací byla součástí všech fází použité projektové metodiky.

Je třeba řešit a pravidelně přezkoumávat dopady bezpečnosti informací ve všech projektech. Odpovědnosti za bezpečnost informací je třeba definovat a přidělit stanoveným rolím definovaným metodami řízení projektů.

Časová náročnost: 4 hodiny

A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení.

A.6.2.1 Politika mobilních zařízení

Opatření: K řízení rizik zavedených používáním mobilních zařízení by měla být přijata politika a podpůrná bezpečnostní opatření.

Implementace: Zajistit pravidla pro používání mobilních zařízení, aby nebyly kompromitovány informace týkající se činnosti organizace. Politika mobilních zařízení by měla brát v úvahu rizika práce s mobilními zařízeními v nechráněných prostředích, např.:

a) registraci mobilních zařízení,
b) požadavky na fyzickou ochranu,
c) omezení instalaci software,
d) požadavky aktuálnost operačního systému mobilního zařízení,
e) řízení přístupu,
f) kryptografické techniky,
g) ochranu před malwarem,
h) vzdálenou deaktivaci, výmaz nebo zablokování,
i) zálohy.

Firemní standardem společnosti v oblasti mobilních zařízení jsou produkty společnosti Apple, jejíž softwarové nástroje zajišťují jak kryptografické techniky, tak vzdálenou deaktivaci, výmaz a zablokování, a také zálohy.

Pro vylepšení zabezpečení mobilních zařízení doporučuji software ESET Mobile Device Management pro Apple iOS, který:

- vylepšuje zabezpečení zařízení s iOS: iPhonů a iPadů,
- obsahuje Anti-Theft ochranu, která umožňuje vzdáleně smazat všechna data,

- podporuje vzdálenou změnu nastavení včetně změn Exchange, Wi-Fi a VPN účtů,
- umožňuje kontrolu vstupního hesla a iCloudu,
- umožňuje nastavení zařízení, soukromí a omezení,
- realizuje vzdálená správu pomocí nástroje ESET Remote Administrator. [9]

Politiku mobilních zařízení bych definoval např. jako doporučení pro práci s mobilními zařízeními, která bych doplnil o postup při ztrátě nebo odcizení mobilního zařízení. Ostatní požadavky na mobilní zařízení by byly implementovány a vynucovány pomocí výše zmíněného software.

Časová náročnost: 16 hodin

Poznámka: ESET Mobile Device Management je součástí balíku ESET Secure Business, který navrhuji k zakoupení v rámci opatření A.12.2.1, zakoupení licence tedy není třeba.

4.4.2 A.7 Bezpečnost lidských zdrojů

A.7.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi svých povinností, a zajistit, aby je plnili.

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Všichni zaměstnanci organizace a tam, kde je to vhodné, i smluvní strany by měli získat odpovídající povědomí o bezpečnosti informací formou vzdělávání a školení a pravidelných aktualizací politik a postupů organizace, dle významu pro zastávanou pracovní funkci.

Implementace: Program budování bezpečnostního povědomí musí být ustaven v souladu s politikami organizace v oblasti bezpečnosti informací a příslušnými postupy. Musí brát v úvahu informace organizace, které mají být chráněny, a opatření, která byla na ochranu informací zavedena.

V návaznosti na kap. 2.7.3, která tuto problematiku teoreticky pokrývá, budu při zavádění budování bezpečnostního povědomí ve společnosti postupovat dle plánu uvedeného v již zmíněné kapitole.

1. Vzhledem k velikosti společnosti (30 zaměstnanců) zvolím centralizovaný způsob řízení bezpečnostních školení, což znamená, že budováním bezpečnostního povědomí bude pověřen pracovník CISO.
2. Rozdělím uživatele do skupin dle jejich znalostí v oblasti bezpečnosti a každé skupině navrhnu patřičné cíle, kterých mají členové vzděláváním dosáhnout.
3. Pro každou skupinu vytvořím školící materiály s ohledem na znalosti a cíle vzdělávání jejich členů.
4. Sestavím plán vzdělávání – určím bezpečnostní problematiku, kterou se budou jednotlivé skupiny při školeních zabývat.
5. Budu dokumentovat průběh jednotlivých školení a sbírat zpětnou vazbu od účastníků, na jejímž základě budu zlepšovat výukové materiály.
6. Určím četnost opakování bezpečnostních školení a četnost aktualizace materiálů.
7. Při dosažení určitých milníku (např. dokončení daného běhu školení, nebo jednou ročně) kriticky zhodnotím průběh a výsledky bezpečnostních školení. Na základě těchto pravidelných zpětných hodnocení budu bezpečnostní školení zlepšovat.

Ve společnosti dále zavedu „měsíčník informační bezpečnosti“, což bude hromadný e-mail všem pracovníkům, který bude obsahovat fakta, rady nebo zásady z oblasti bezpečnosti.

Příklad obsahu hromadného e-mailu rozesílaného všem zaměstnancům společnosti:

- používejte silná hesla,
- pravidelně zálohujte svá data,
- neotvírejte e-mailové přílohy od osob, které neznáte,
- když odcházíte od počítače, uzamkněte jej,
- podezření na narušení bezpečnosti ihned hlaste.

Časová náročnost: 24 hodin

A.7.2.3 Disciplinární řízení

Opatření: Měl by existovat formální disciplinární proces, oznámený všem, pro podniknutí kroků vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Implementace: Zavést v organizaci formální disciplinární proces, který zajistí správné a spravedlivé zacházení pro zaměstnance, kteří jsou podezřelí z narušení bezpečnosti informací. Měl by stanovit odstupňované reakce, které berou v úvahu například:

a) povahu a závažnost narušení a jeho vliv na podnikatelské aktivity,
b) zda se jedná o opakovaný přestupek,
c) zda byl či nebyl narušitel řádně vyškolen,
d) obchodní smlouvy a další smlouvy dle nutnosti.

Disciplinární proces byl měl být v organizaci použit jako odstrašující prostředek odrazující zaměstnance z porušení politik a postupů organizace v oblasti bezpečnosti informací. Disciplinární proces by neměl být zahájen bez předchozího ověření, že došlo k narušení bezpečnosti informací.

Časová náročnost: 6 hodin

4.4.3 A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti za přiměřenou ochranu.

A.8.1.3 Přípustné použití aktiv

Opatření: Měla by být identifikována, dokumentována a implementována pravidla pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací.

Implementace: Seznámit zaměstnance a externí uživatele používající nebo mající přístup k aktivům organizace o požadavcích bezpečnosti informací na daná aktiva organizace. Zaměstnanci a externí uživatele používající nebo mající přístup k aktivům organizace být měli být odpovědní za použití jakýchkoliv zdrojů pro zpracování informací a jakéhokoliv podobného použití provedeného v rámci své odpovědnosti.

Časová náročnost: 6 hodin

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci.

A.8.2.3 Manipulace s aktivy

Opatření: Pro zacházení s aktivy by měly být vytvořeny a zavedeny postupy v souladu se schématem klasifikace informací přijatým organizací.

Implementace: Vypracovat a zavést postupy pro zacházení, zpracování, ukládání a předávání informací v souladu s jejich klasifikací, přičemž je třeba brát v úvahu:

a) omezení přístupu podporující požadavky na ochranu na každé úrovni klasifikace,
b) udržování formálního záznamu o oprávněných příjemcích aktiv,
c) ochranu dočasných nebo trvalých kopií informace na úrovni odpovídající ochraně původní informace,
d) skladování IT aktiv v souladu se specifikacemi výrobce,
e) zřetelné označení všech kopií médií pro upoutání pozornosti oprávněného příjemce.

Časová náročnost: 4 hodiny

4.4.4 A.9 Řízení přístupu

A.9.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systémům a službám.

A.9.2.3 Správa privilegovaných přístupových práv

Opatření: Přidělení a použití privilegovaných přístupových práv by mělo být omezeno a řízeno.

Implementace: Při řízení privilegovaných přístupových práv prostřednictvím formálního procesu autorizace:

a) identifikovat privilegovaná přístupová práva a aplikace nebo uživatel, kterým je potřeba tyto práva přidělit,
b) přidělovat přístupová práva na základě minimální potřeby pro jejich provozní role,
c) udržovat proces autorizace a záznam všech přidělených privilegií,
d) pravidelně přezkoumávat kompetence uživatelů s privilegovanými přístupovými právy.

Časová náročnost: 4 hodiny

A.9.2.5 Přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv by měli v pravidelných intervalech přezkoumávat přístupová práva uživatelů.

Implementace: Při přezkoumávání přístupových práv uživatelů je třeba:

a) přezkoumávat práva uživatelů v pravidelných intervalech a po každé změně pracovní pozice uživatele (zaměstnance) nebo ukončení pracovního poměru,
b) zaznamenávat změny týkající se privilegovaných účtů formou logu.

Časová náročnost: 2 hodiny

A.9.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu svých autentizačních informací.

A.9.3.1 Používání tajných autentizačních informací

Opatření: Po uživatelích by mělo být vyžadováno, aby při používání tajných autentizačních informací dodržovali postupy organizace.

Implementace: Poučit všechny uživatele, aby:

a) udržovali tajnou autentizační informaci jako důvěrnou, a zajistili, že není vyzrazena žádným jiným stranám,
b) se vyhnuli uchovávání záznamu autentizační informace (např. na papíre, v nezabezpečeném textovém souboru), kromě případů, kdy je autentizační informace uchováván způsobem, který byl schválen vedením organizace (např. trezor s heslem),
c) změnili tajnou autentizační informaci v případě, že se vyskytne jakýkoliv náznak její možné kompromitace,
d) pokud jsou jako tajné autentizační informace používána hesla, zvolili hesla, která:
    a. jsou snadno zapamatovatelná,
    b. nejsou založena na osobních informacích (např. jména, data narození atd.),
    c. neobsahující po sobě jdoucí číselné nebo abecední znaky,
e) nepoužívali stejnou autentizační informaci pro přístup k různým informačním systémům, aplikacím nebo službám.

Doporučuji zajistit změnu uživatelských hesel v pravidelných intervalech, např. 1 ročně.

Časová náročnost: 2 hodiny

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: Zabránit neoprávněnému přístupu k systémům a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Opatření: Přístup k informacím a funkcím aplikačních systémů by měl být omezen v souladu s politikou řízení přístupu.

Implementace: S cílem podpořit požadavky na omezení přístupu vzít v úvahu:

a) poskytování prostředků pro kontrolu přístupu k funkcím aplikačního systému,
b) kontrolování, ke kterým datům může konkrétní uživatel přistupovat,
c) kontrolování přístupových práv uživatelů (např. práv číst, zapisovat, mazat),
d) kontrolování přístupových práv jiných aplikací,
e) omezování informací obsažených ve výstupech,
f) zajištění fyzického neb logického řízení přístupu pro izolaci citlivých aplikací, dat nebo systémů.

Časová náročnost: 3 hodiny

4.4.5 A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/nebo integrity informací.

A.10.1.1 Politika pro použití kryptografických opatření

Opatření: Měla by být vypracována a realizována politika použití kryptografických opatření na ochranu informací.

Implementace: Vypracovat politiky v oblasti kryptografie a při jejich tvorbě zvážit např.:

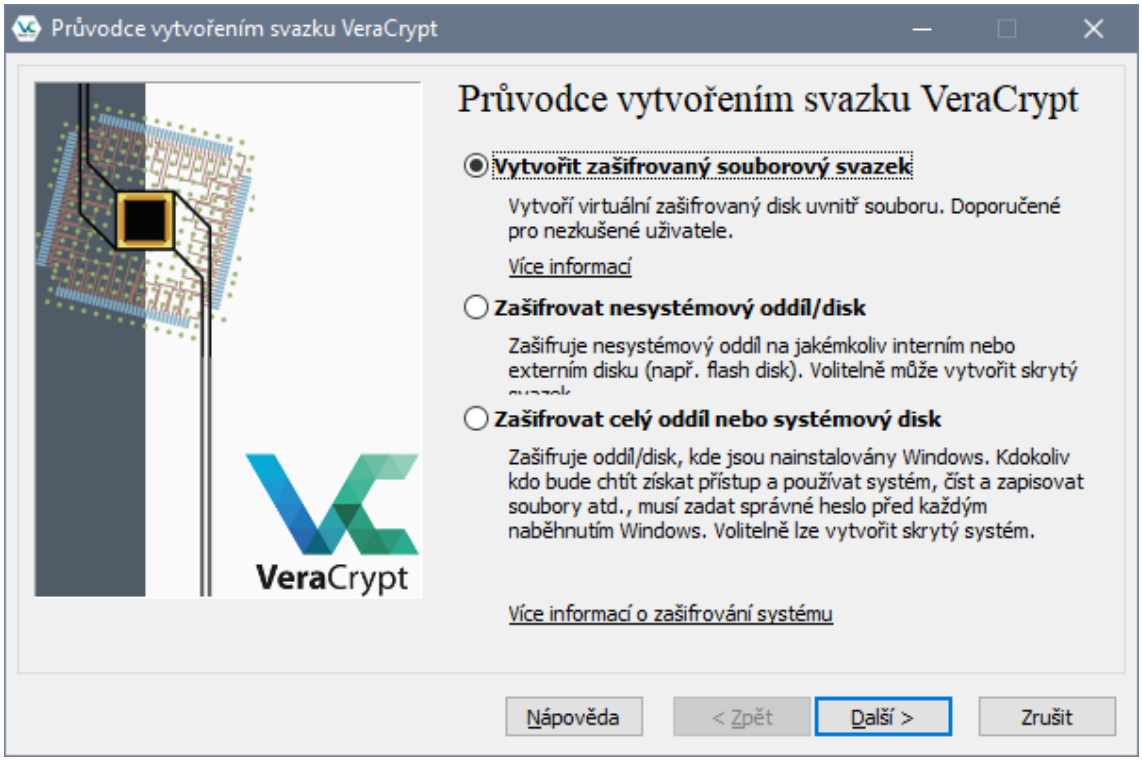
- manažerský přístup ve vztahu k používání kryptografických opatření v rámci celé organizace, včetně obecných zásad, podle nichž by měly být informace chráněny,
- určit vyžadovanou úroveň ochrany s ohledem na typ, sílu a kvalitu požadovaného šifrovacího algoritmu,

- přístup ke správě klíčů a metody obnovení zašifrované informace v případě ztráty, kompromitace nebo poškození klíčů,
- role a zodpovědnosti (implementace politiky, správa klíčů).

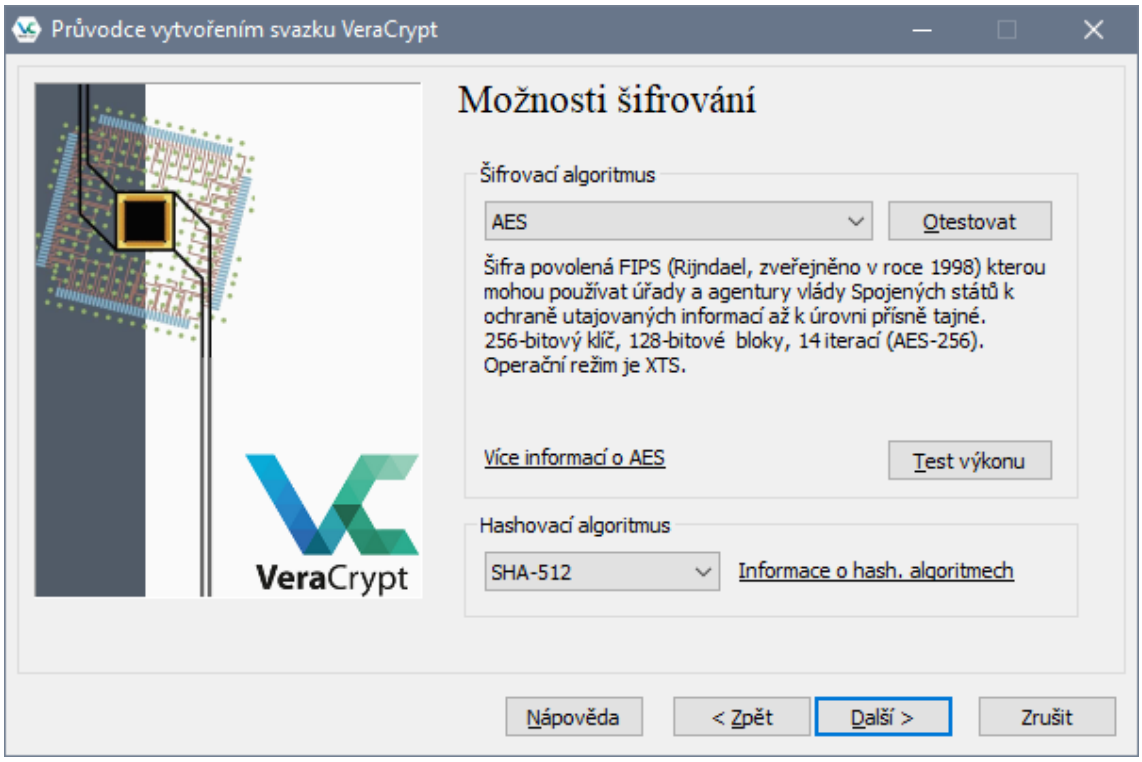
Kryptografická opatření lže použít pro dosažení různých cílů v oblasti bezpečnosti informací, například:

- důvěrnosti – pomocí šifrování citlivých nebo kritických informací,
- integrity/autenticity – např. pomocí digitálních podpisů,
- autentizace – použitím kryptografických technik k autentizaci uživatelů a dalších entit systému žádajících o přístup k uživatelům, entitám a zdrojům systému.

Pro šifrování doporučuji použít open-source nástroj VeraCrypt, který je nástupcem oblíbeného šifrovacího nástroje TrueCrypt, jehož vývoj byl ukončen. VeraCrypt je softwarový nástroj, který umožňuje vytvoření a uchovávání „za běhu“ šifrovaných oddílů. Šifrování „za běhu“ znamená, že data jsou před uložením automaticky šifrována a před načtením automaticky dešifrována, a to bez nutnosti jakéhokoliv zásadu ze strany uživatele. [10]



Obrázek 17: Ukázka vytvoření svazku VeraCrypt (Zdroj: vlastní zpracování)



Obrázek 18: Ukázka možností šifrování svazku VeraCrypt (Zdroj: vlastní zpracování)

Časová náročnost: 6 hodin

V další etapě je vhodné zavést opatření A.10.1.2 Správa klíčů, aby byla opatření v oblasti kryptografie kompletní.

4.4.6 A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.2 Zařízení

Cíl: Zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace.

A.11.2.2 Podpůrné služby

Opatření: Zařízení by mělo být chráněno před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb.

Implementace: Pro zajištění funkčnosti podpůrných služeb (např. elektřina, telekomunikace, klimatizace atd.):

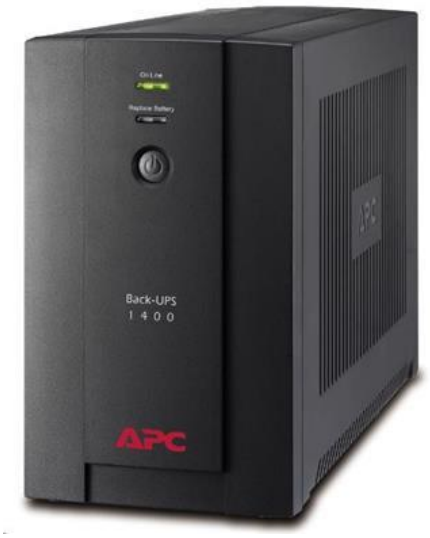
a) zajistit pravidelné posuzování a testování vybavení zajišťujícího podpůrné služby z hlediska schopnosti vyhovět potřebám organizace,

b) zajistit včasné zjištění případné závady (např. varovným zvukovým signálem),
c) implementovat např. vícenásobné přívody s odlišnými fyzickými trasami.

Doporučuji zřídit redundantní internetové připojení, které se použije při výpadku primárního, kabelového připojení. Navrhuji tedy zřízení záložního bezdrátového internetového připojení od společnosti T-Mobile s následujícími parametry:

Obrázek 19: Redundantního internetového připojení (Převzato z [11])

Aby byl zachován provoz serverů a dostupnost serverů z internetu při výpadku elektřiny, navrhuji implementovat záložní zdroj nepřerušovaného napájení (UPS) k napájení serverů a síťových prvků, např. APC BX1400U.



Obrázek 20: Zdroj nepřerušovaného napájení APC BX1400U (Převzato z [12])

Časová náročnost: 12 hodin

Náklady: Redundantní připojení k internetu – 599 Kč/měsíc (7 188 Kč/rok),

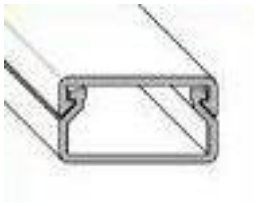
zdroj nepřerušovaného napájení (UPS) – 3 819 Kč.

A.11.2.3 Bezpečnost kabelových rozvodů

Opatření: Silová a telekomunikační kabeláž určená pro přenos dat nebo podpůrných informačních služeb by měla být chráněna před odposloucháváním, rušením nebo poškozením.

Implementace: Pro odpovídající ochranu kabeláže:

a) je-li to možné, vést napájecí a telekomunikační linky připojené k vybavení pro zpracování informací pod podlahou, ve zdi nebo je odpovídajícím způsobem chránit (např. kabelážními lištami),
b) zajistit implementaci zvláštních opatření pro citlivé nebo kritické systémy (např. uzamykatelné rozvodné skříně).



Obrázek 21: MALPRO EIP 18x13 instalační lišta vkládací (Převzato z [13])

Časová náročnost: 8 hodin

Náklady: MALPRO EIP 18x13 instalační lišta vkládací – 1100 Kč/100 metrů.

A.11.2.8 Uživatelská zařízení bez obsluhy

Opatření: Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaného zařízení.

Implementace: Poučit uživatele o bezpečnostních požadavcích a postupech pro ochranu neobsluhovaných zařízení a o jejich odpovědnosti za realizaci této ochrany. Informovat uživatele, aby:

a) ukončovali aktivní relace po dokončení činnosti, pokud nemohou být zabezpečeny jiným způsobem (např. spořičem obrazovky s heslem),
b) se odhlašovali z aplikací nebo síťových služeb, pokud je již nepoužívají,
c) zabezpečovali počítače nebo mobilní zařízení před neoprávněným použitím pomocí zámku nebo rovnocenným opatřením (např. přístupovým heslem).

Časová náročnost: 1 hodina

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Pro vybavení pro zpracování informací by měla být přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií, a zásada prázdné obrazovky.

Implementace: Zásada prázdného stolu a obrazovky musí brát v úvahu klasifikaci informací, zákonné a smluvní požadavky, odpovídající rizika. V rámci zásady prázdného stolu a obrazovky je třeba zajistit, aby:

a) citlivé nebo kritické informace organizace, v papírové nebo elektronické formě, byly uzamčeny, pokud nejsou využívány,
b) počítače nebo terminály byly ponechávány s odhlášenými uživateli, nebo s mechanismem zamykajícím obrazovku, který je opatřen heslem,
c) bylo zabráněno neoprávněnému použití tiskáren, kopírek a dalších reprodukčních technologií.

Časová náročnost: 1 hodina

4.4.7 A.12 Bezpečnost provozu

A.12.2 Ochrana proti malwaru

Cíl: Zajistit, že informace a vybavení pro zpracování informací jsou před malwarem chráněny.

A.12.2.1 Opatření proti malwaru

Opatření: Měla by být implementována opatření pro detekci, prevenci a zotavení na ochranu před malwarem, v kombinaci s vhodným zvyšováním povědomí uživatelů.

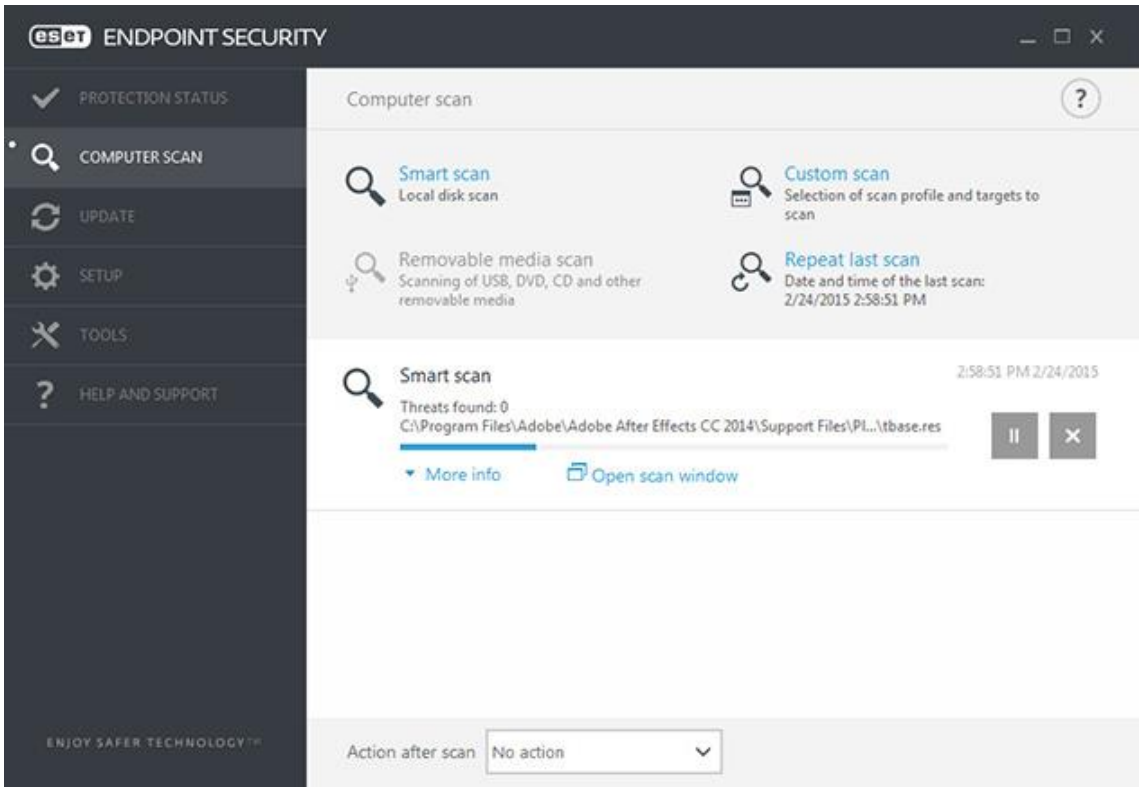
Implementace: Postavit ochranu před malwarem na detekci malwaru, aktualizacích softwaru, na povědomí o bezpečnosti informací a odpovídajících opatřeních v oblasti přístupu k systému. Je třeba zvážit:

- stanovení formální politiky zakazující používání neautorizovaného softwaru,
- implementaci opatření, která zabraňují nebo detekují používání známých nebo podezřelých škodlivých webových stránek,
- pravidelnou instalaci aktualizací softwaru pro detekci malwaru,
- skenování souborů na přítomnost malware,

- definování plánu kontinuity podnikání pro zotavení se z útoku vyvolaného malwarem (viz. A.12.3),
- zřízení izolovaného prostředí, ve kterém mohou nastat katastrofické účinky.

Doporučuji nasazení software ESET Endpoint Security, který:

- poskytuje komplexní ochrana koncových stanic se systémem Windows,
- je optimalizován pro virtuální prostředí – chrání před útoky i virtuální stroje,
- umožňuje filtrování přístupu na webové stránky a síťová zařízení,
- podporuje vzdálenou správu pomocí nástroje ESET Remote Administrator. [14]



Obrázek 22: Ukázka prostředí ESET Endpoint Security (Převzato z [14])

Časová náročnost: 12 hodin

Náklady: Balík ESET Secure Business – 7 472 Kč/rok.

Poznámka: V balíku ESET Secure Business je zahrnuta jak licence na ESET Endpoint Security, tak licence na ESET Mobile Device Management (viz opatření A.6.2.1).

A.12.3 Zálohování

Cíl: Ochrana před ztrátou dat.

A.12.3.1 Zálohování informací

Opatření: Pravidelně by měly být pořizovány a testovány záložní kopie informací, softwaru a bitových kopií systému v souladu se schválenou politikou zálohování.

Implementace: Stanovit politiku zálohování definující požadavky organizace na zálohování informací, softwaru a systémů, která bude zahrnovat požadavky na uchovávání a ochranu. Při vytváření, resp. revizi plánu zálohování vzít v úvahu např.:

- vedení přesných a úplných záznamů o záložních kopiích a dokumentovaných postupů obnovy,
- rozsah a četnost zálohování by měly odrážet požadavky vyplývající z činností organizace a kritičnost informací z hlediska kontinuity činností organizace,
- záložní informace by měly být uloženy na jiném místě, než je sídlo společnosti, aby na nich havárie hlavního sídla nezpůsobila škody,
- záložním informacím by měla být poskytnuta odpovídající úroveň fyzické ochrany,
- záložní média by měla být pravidelně testována, aby se zajistilo jejich spolehlivé použití v případě nouzové situace.

Doporučuji zavést mechanismy, které zajistí, že opatření pro zálohování jednotlivých informací, systémů a služeb budou pravidelně kontrolována, aby bylo zajištěno splnění požadavků plánů kontinuity činností organizace. Pro kritické informace organizace je navíc třeba stanovit doba uchování s přihlédnutím k případným požadavkům na trvalé uchování archivních kopií.

Časová náročnost: 10 hodin

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a generovat důkazy.

A.12.4.1 Zaznamenávání událostí formou logů

Opatření: Musí být pořizovány a pravidelně přezkoumávány záznamy událostí formou logů zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.

Implementace: Záznamy událostí formou logů by měly, je-li to vhodné, obsahovat např.:

- ID uživatele,
- činnosti systému,
- datum, čas a podrobnost důležitých událostí (např. přihlášení, odhlášení),
- identitu, umístění zařízení a identifikátor systému,
- záznamy o úspěšných a odmítnutých pokusech o přístup k systému nebo datům,
- změny konfigurace systému,
- použití privilegií, systémových nástrojů a aplikací,
- seznam souborů, ke kterým bylo přistupováno a typ přístupu (čtení, zápis atd.),
- síťové adresy a protokoly,
- poplachy vyvolané systémem řízení přístupu.

Správci systému by neměli mít oprávnění měnit nebo mazat záznamy o svých vlastních aktivitách.

V případě, že se vedení společnosti rozhodne toto opatření zavést a bude ochotné jej patřičně zafinancovat, doporučuji nákup softwaru pro logování, nákup kompatibilního hardware a vytvoření pracovní pozice pro datového analytika, který se bude logováním v organizaci zabývat. V opačném případě může být opatření v určité míře realizováno pomocí stávajících prostředků podporujících zaznamenávání činností formou logů, z čehož jsem také vycházel při odhadu časové náročnosti a nákladů na zavedení opatření.

V dalších etapách je třeba zavést opatření, která zaznamenávání událostí formou logů podporují, aby byla zajištěna autenticita a integrita zaznamenaných událostí:

- A.12.4.2 Ochrana logů
- A.12.4.3 Logy o činnosti administrátorů a operátorů
- A.12.4.4 Synchronizace hodin

Časová náročnost: 8 hodin

4.5 Aplikovatelnost navržených opatření

Označení „ANO“ ve sloupci „Vyloučeno“ je uvedeno u opatření z přílohy A normy ISO/IEC 27001, která zavedena nebudou, protože pro společnost nejsou relevantní. Označení „NE“ ve sloupci „Vyloučeno“ je uvedeno u opatření, jejichž zavedení bude realizováno dle návrhu v předchozí kapitole.

Tabulka 11: Aplikovatelnost navržených opatření (Zdroj: vlastní zpracování)

Bezpečnostní opatření		Vyloučeno
A.5	**Politiky bezpečnosti informací**	ANO
A.6	**Organizace bezpečnosti informací**	
A.6.1	**Interní organizace**	
A.6.1.1	Role a odpovědnosti bezpečnosti informací	NE
A.6.1.2	Princip oddělení povinností	NE
A.6.1.3	Kontakt s příslušnými orgány a autoritami	NE
A.6.1.4	Kontakt se zájmovými skupinami	NE
A.6.1.5	Bezpečnost informací v řízení projektů	NE
A.6.2	**Mobilní zařízení a práce na dálku**	
A.6.2.1	Politika mobilních zařízení	NE
A.6.2.2	Práce na dálku	ANO
A.7	**Bezpečnost lidských zdrojů**	
A.7.1	**Před vznikem pracovního vztahu**	ANO
A.7.2	**Během pracovního vztahu**	
A.7.2.1	Odpovědnosti vedení organizace	ANO
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	NE
A.7.2.3	Disciplinární řízení	NE
A.7.3	**Ukončení a změna pracovního vztahu**	ANO
A.8	**Řízení aktiv**	
A.8.1	**Odpovědnost za aktiva**	
A.8.1.1	Seznam aktiv	ANO
A.8.1.2	Vlastnictví aktiv	ANO
A.8.1.3	Přípustné použití aktiv	NE
A.8.1.4	Navrácení aktiv	ANO
A.8.2	**Klasifikace informací**	
A.8.2.1	Klasifikace informací	ANO
A.8.2.2	Označování informací	ANO
A.8.2.3	Manipulace s aktivy	NE
A.8.3	**Manipulace s médii**	ANO
A.9	**Řízení přístupu**	
A.9.1	**Požadavky organizace na řízení přístupu**	ANO

A.9.2	**Řízení přístupu uživatelů**	
A.9.2.1	Registrace a zrušení registrace uživatele	ANO
A.9.2.2	Správa uživatelských přístupů	ANO
A.9.2.3	Správa privilegovaných přístupových práv	NE
A.9.2.4	Správa tajných autentizačních informací uživatelů	ANO
A.9.2.5	Přezkoumání přístupových práv uživatelů	NE
A.9.2.6	Odebrání nebo úprava přístupových práv	ANO
A.9.3	**Odpovědnosti uživatelů**	
A.9.3.1	Používání tajných autentizačních informací	NE
A.9.4	**Řízení přístupu k systémům a aplikacím**	
A.9.4.1	Omezení přístupu k informacím	NE
A.9.4.2	Bezpečné postupy přihlášení	ANO
A.9.4.3	Systém správy hesel	ANO
A.9.4.4	Použití privilegovaných programových nástrojů	ANO
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	ANO
A.10	**Kryptografie**	
A.10.1	**Kryptografická opatření**	
A.10.1.1	Politika pro použití kryptografických opatření	NE
A.10.1.2	Správa klíčů	ANO
A.11	**Fyzická bezpečnost a bezpečnost prostředí**	
A.11.1	**Bezpečné oblasti**	
A.11.1.1	Fyzický bezpečnostní perimetr	ANO
A.11.1.2	Fyzické kontroly vstupu	NE
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	ANO
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	ANO
A.11.1.5	Práce v bezpečných oblastech	ANO
A.11.1.6	Oblasti pro nakládku a vykládku	ANO
A.11.2	**Zařízení**	
A.11.2.1	Umístění zařízení a jeho ochrana	ANO
A.11.2.2	Podpůrné služby	ANO
A.11.2.3	Bezpečnost kabelových rozvodů	NE
A.11.2.4	Údržba zařízení	ANO
A.11.2.5	Přemístění aktiv	ANO
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	ANO
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	ANO
A.11.2.8	Uživatelská zařízení bez obsluhy	NE
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	NE
A.12	**Bezpečnost provozu**	
A.12.1	**Provozní postupy a odpovědnosti**	ANO
A.12.2	**Ochrana proti malwaru**	
A.12.2.1	Opatření proti malwaru	NE

A.12.3	**Zálohování**	
A.12.3.1	Zálohování informací	NE
A.12.4	**Zaznamenávání formou logů a monitorování**	
A.12.4.1	Zaznamenávání událostí formou logů	NE
A.12.4.2	Ochrana logů	ANO
A.12.4.3	Logy o činnosti administrátorů a operátorů	ANO
A.12.4.4	Synchronizace hodin	ANO
A.12.5	**Správa provozního softwaru**	ANO
A.12.6	**Řízení technických zranitelností**	ANO
A.12.7	**Hlediska auditu informačních systémů**	ANO
A.13	**Bezpečnost komunikací**	ANO
A.14	**Akvizice, vývoj a údržba systémů**	ANO
A.15	**Dodavatelské vztahy**	ANO
A.16	**Řízení incidentů bezpečnosti informací**	ANO
A.17	**Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací**	ANO
A.18	**Soulad s požadavky**	ANO

Prohlášení o aplikovatelnosti naleznete v příloze.

4.6 Obecné nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation) nabývá účinnosti dne 25. května 2018 a platí pro všechny organizace nabízející zboží nebo služby v rámci EU a manipulující s osobními údaji subjektů (fyzických osob). Jedná se o účinné nařízení EU, což znamená, že má přednost před národní legislativou.

Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. [15]

Obecné nařízení o ochraně osobních údajů ukládá správcům osobních údajů např.:

- povinnost zabezpečit zpracování osobních údajů,
- povinnost provádět posouzení vlivu na ochranu osobních údajů,

- povinnost ohlašovat porušení zabezpečení osobních údajů, tzv. data breaches (jak dozorovému úřadu, tak subjektu údajů),
- povinnost jmenovat pověřence pro ochranu osobních údajů,
- povinnost vést záznamy o činnostech zpracování osobních údajů (včetně povinnosti zaznamenávat i přístupy ke čtení osobních údajů). [15]

Subjekt údajů (fyzická osoba) má dle tohoto nařízení např.:

- právo na přístup k osobním údajům,
- právo na opravu nebo výmaz („právo být zapomenut“),
- právo na omezení zpracování,
- právo na přenositelnost údajů,
- právo vznést námitku. [15]

Splnění požadavků, které Obecné nařízení o ochraně osobních údajů vyžaduje, napomáhají např. následující opatření navržená k zavedení v první etapě:

- A.6.1.1 Role a odpovědnosti bezpečnosti informací,
- A.6.1.3 Kontakt s příslušnými orgány a autoritami,
- A.9.2.5 Přezkoumání přístupových práv uživatelů,
- A.9.4.1 Omezení přístupu k informacím,
- A.12.4.1 Zaznamenávání událostí formou logů.

4.7 Údržba, přezkoumání, zlepšování

Zajištění bezpečnosti informací je nikdy nekončící proces, který je třeba neustále zlepšovat. Aby bylo možné aktiva účinně chránit např. vůči novým hrozbám, je vhodné rizika pravidelně přezkoumávat a patřičně modifikovat bezpečnostní opatření pro jejich ochranu.

Pravidelnou údržbu, přezkoumání a zlepšování informační bezpečnosti ve společnosti zajistím pomocí interního systému řízení požadavků a služeb, který bude automaticky vytvářet a přidělovat k řešení servisní požadavky pracovníkovi CISO v určitých časových intervalech, po prvotním zavedení bezpečnostních opatření např. jednou ročně. Určení vyhovujících časových intervalů a obsahu pravidelných kontrol bude probíhat až na základě reálných poznatků z provozu.

4.8 Ekonomické zhodnocení a časový plán

Při výpočtu nákladů na lidské zdroje jsem vycházel z předpokládané hodinové mzdy specialisty bezpečnosti informací s minimálně dvouletou praxí, který je interním zaměstnancem společnosti, ve výši 400 Kč/h.

V případě, že by se společnost rozhodla využít pro návrh a zavedení opatření služeb třetí strany, hodinová mzda specialisty bezpečnosti informací by byla minimálně 800 Kč/h.

Časová náročnost v tabulkách je uváděna v hodinách, náklady pak v českých korunách.

4.8.1 Náklady na návrh opatření

Tabulka 12: Náklady na návrh opatření (Zdroj: vlastní zpracování)

Návrh opatření	Časová náročnost	Celkové náklady
Rozsah a hranice	8	3 200 Kč
Analýza rizik	56	22 400 Kč
Akceptace rizik	6	2 400 Kč
Návrh opatření pro zvládání rizik	48	19 200 Kč
Aplikovatelnost navržených opatření	16	6 400 Kč
Obecné nařízení o ochraně osobních údajů	8	3 200 Kč
Údržba, přezkoumání, zlepšování	6	2 400 Kč
Celkem	**148**	**59 200 Kč**

Časová náročnost návrhu bezpečnostních opatření byla 148 hodin, z čehož vyplývají celkové náklady na práci specialisty bezpečnosti informací ve výši 59 200 Kč.

4.8.2 Náklady na zavedení (údržbu) opatření (první etapa)

Tabulka 13: Náklady na zavedení (údržbu) opatření (Zdroj: vlastní zpracování)

Opatření	Časová náročnost		Náklady		Celkové náklady	
	Zavedení	Ročně	Zavedení	Ročně	Zavedení	Ročně
A.6.1.1	16	2	15 000 Kč		21 400 Kč	800 Kč
A.6.1.2	4	1			1 600 Kč	400 Kč
A.6.1.3	4	1			1 600 Kč	400 Kč
A.6.1.4	2	1			800 Kč	400 Kč
A.6.1.5	4	1			1 600 Kč	400 Kč
A.6.2.1	16	3			6 400 Kč	1 200 Kč
A.7.2.2	24	8			9 600 Kč	3 200 Kč
A.7.2.3	6	1			2 400 Kč	400 Kč
A.8.1.3	6	1			2 400 Kč	400 Kč
A.8.2.3	4	1			1 600 Kč	400 Kč
A.9.2.3	4	1			1 600 Kč	400 Kč
A.9.2.5	2	1			800 Kč	400 Kč
A.9.3.1	2	1			800 Kč	400 Kč
A.9.4.1	3	1			1 200 Kč	400 Kč
A.10.1.1	6	1			2 400 Kč	400 Kč
A.11.2.2	12	1	11 007 Kč	7 188 Kč	15 807 Kč	7 588 Kč
A.11.2.3	8	0	1 100 Kč		4 300 Kč	0 Kč
A.11.2.8	1	0			400 Kč	0 Kč
A.11.2.9	1	0			400 Kč	0 Kč
A.12.2.1	12	3	7 472 Kč	7 472 Kč	12 272 Kč	8 672 Kč
A.12.3.1	10	2			4 000 Kč	800 Kč
A.12.4.1	8	2			3 200 Kč	800 Kč
Celkem	**155**	**33**	**34 579 Kč**	**14 660 Kč**	**96 579 Kč**	**27 860 Kč**

Součtem nákladů na práci specialisty bezpečnosti informací a nákladů na zavedení jednotlivých opatření jsem získal celkovou částku potřebnou pro zavedení navržených opatření pro zvládání největších rizik ve výši 96 579 Kč.

Odhadl jsem také časovou náročnost a roční náklady na údržbu již zavedených opatření ve výši 27 860 Kč, z čehož většinové náklady tvoří platba redundantního internetového připojení a softwarové licence.

Uvedené časové náročnosti a náklady jsou pouze mým kvalifikovaným odhadem.

4.8.3 Celkové náklady na návrh a zavedení opatření (první etapa)

Tabulka 14: Náklady na návrh a zavedení opatření (Zdroj: vlastní zpracování)

Návrh a zavedení opatření	Časová náročnost	Celkové náklady
Návrh bezpečnostních opatření	148	59 200 Kč
Zavedení bezpečnostních opatření	155	96 579 Kč
Celkem	**303**	**155 779 Kč**

Součtem nákladů na návrh a odhadovaných nákladů na zavedení opatření jsem zjistil částku potřebnou pro návrh a zavedení opatření pro zvládání největších rizik ve výši 155 779 Kč.

V tabulkách pro zjednodušení úmyslně zanedbávám režijní náklady na stávající zaměstnance. Zaměstnanci se na návrhu a zavedení opatření podílejí nejčastěji formou konzultací, které zahrnují například:

- komunikaci s vedením společnosti nebo jinými zaměstnanci,
- spolupráci vlastníků (garantů) aktiv při analýze rizik nebo návrhu opatření,
- komunikaci se zaměstnanci a zjišťování informací o již zavedených bezpečnostních opatření,
- spolupráci zaměstnanců při zavádění navržených bezpečnostních opatření.

4.8.4 Časová náročnost zavedení bezpečnostních opatření (první etapa)

Časová náročnost zavedení navržených bezpečnostních opatření je odhadována na 155 hodin, což je za předpokladu 8 hodinového pracovního dne přibližně 20 pracovních dní.

Zavedení některých opatření již bylo úplně nebo částečně realizováno (např. tvorba nebo úprava již existujících politik, směrnic nebo dokumentace). Dokončení zavedení již částečně implementovaných opatření a zavedení ostatních opatření navržených do první etapy zavádění (zvláště pak těch spojených s náklady na zavedení) je naplánováno do konce roku 2017.

5 ZHODNOCENÍ A PŘÍNOSY PRÁCE

V rámci představení a přiblížení oblasti podnikání společnosti jsem zmapoval hlavní podnikové procesy, které bude možné opět použít např. při implementaci dalších norem.

Zavedením bezpečnostních opatření na ochranu informací získá společnost konkurenční výhodu, protože žádná z analyzovaných konkurenčních společností nemá zaveden systém řízení bezpečnosti informací (ISMS) nebo není certifikována dle ISO/IEC 27001.

V rámci opatření A.7.2.2 (Povědomí, vzdělávání a školení bezpečnosti informací) jsem navrhl plán budování bezpečnostního povědomí, jehož realizací a následným zlepšováním se docílí zvýšení bezpečnostního povědomí u zaměstnanců a zvýšení bezpečnosti informací ve společnosti.

Ke zvýšení informační bezpečnosti dojde nejen zavedením opatření navržených na základě analýzy rizik, ale také zavedením bezpečnostních opatření spadajících do oblasti interní organizace bezpečnosti informací (A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4, A.6.1.5), jejichž zavedení přímo nevyplývalo z analýzy rizik, ale k zavedení jsem je přesto navrhl z důvodu jejich obecné působnosti v oblasti bezpečnosti informací.

Zjistil jsem, že v 25. května 2018 nabývá účinnosti Obecné nařízení o ochraně osobních údajů (GDPR), proto jsem v kap. 4.6 uvedl opatření navržená k zavedení, která plnění požadavků tohoto nařízení napomáhají.

V rámci opatření A.12.2.1 (Ochrana proti malwaru) jsem navrhl nasazení software ESET Endpoint Security, který je součástí balíku ESET Secure Business. Tento balík produktů zároveň obsahuje licenci pro produkt ESET Mobile Device Management, který jsem navrhl k zavedení v opatření A.6.2.1 (Politika mobilních zařízení). Oba produkty je možné (a vhodné) vzdáleně spravovat pomocí nástroje ESET Remote Administrator, což umožní efektivnější prosazování bezpečnostních politik a také ulehčí práci správci informačních technologií.

ZÁVĚR

V teoretické části jsem se zabýval základními pojmy z oblasti bezpečnosti informací, Demingovým cyklem, koncepcemi řízení, rámci, metodikami, normalizačními institucemi a normami. Dále jsem se zabýval systémem řízení bezpečnosti informací, jeho etapami, povinnou dokumentací a budováním bezpečnostního povědomí v organizaci. Obecně jsem definoval aktiva, rizika a opatření, u kterých jsem uvedl návaznost na praktickou část práce.

Vypracoval jsem analýzu současného stavu, na jejímž začátku jsem přiblížil společnost, pro kterou jsem návrh zavedení bezpečnostních opatření zpracovával, a také jsem graficky znázornil hlavní podnikové procesy společnosti. Navázal jsem analýzou současného stavu bezpečnosti rozdělenou do tematických celků. Současný stav bezpečnosti jsem kriticky zhodnotil, uvedl jsem očekávání vedení společnosti od této práce a provedl jsem stručnou analýzu konkurenčního prostředí z pohledu informační bezpečnosti.

Ve vlastním návrhu řešení jsem určil hranice a rozsah bezpečnosti informací a vypracoval jsem analýzu rizik, která zahrnuje identifikaci a ohodnocení aktiv a také hrozeb, které na aktiva mohou působit, čímž jsem získal zranitelnost daných aktiv vůči daným hrozbám, z čehož vyplynula rizika pro jednotlivá aktiva. Z analýzy rizik jsem zjistil, že největší riziko představuje ztráta základních služeb, chybné fungování aplikačního programového vybavení, neoprávněné činnosti v podobě poškození dat nebo jejich nezákonného zpracování a také chyba v používání nebo zneužití oprávnění. Na základě rozhodnutí vedení společnosti jsem akceptoval bezvýznamná, akceptovatelná a nízká rizika.

Na základě analýzy rizik jsem navrhl bezpečnostní opatření pro zvládání největších rizik, což jsou nežádoucí a nepřijatelná rizika, která znamenají vážné potíže nebo podstatné finanční ztráty, resp. existenční potíže pro organizaci. Jednotlivá navržená opatření jsem detailně popsal a nastínil, co je potřeba provést a brát v úvahu při jejich implementaci ve společnosti. U vybraných opatření jsem uvedl způsob jejich implementaci v podobě konkrétního řešení. Odhadl jsem časovou náročnost a náklady na implementaci jednotlivých opatření. Zpracoval jsem prohlášení o aplikovatelnosti.

Seznámil jsem se s Obecným nařízením o ochraně osobních údajů (GDPR), které nabývá účinnosti 25. května 2018 a přiblížil jsem povinnosti správců osobních údajů a práva subjektů osobních údajů (fyzických osob), které z něj vyplývají. Při návrhu zavedení bezpečnostních opatření jsem zmíněné nařízení bral v úvahu a věnoval mu samostatnou kapitolu, ve které jsem vyjmenoval navržená opatření, která plnění požadavků tohoto zařízení napomáhají.

Návrh a zavedení bezpečnostních opatření jsem ekonomicky zhodnotil – vyčíslil jsem časovou náročnost a z ní plynoucí náklady na návrh opatření (59 200 Kč). Odhadl jsem časovou náročnost (přibližně 20 pracovních dní) a náklady na zavedení opatření (96 579 Kč). Odhadl jsem také časovou náročnost a roční náklady na pravidelnou údržbu opatření navržených k zavedení (27 860 Kč). Součtem nákladů na návrh a odhadovaných nákladů na zavedení opatření jsem dostal částku 155 779 Kč, která je pro návrh a zavedení opatření pro zvládání největších rizik (těch s největším dopadem) potřebná.

Práci jsem dále zhodnotil a nastínil její přínosy, mezi které patří např. zmapování hlavních podnikových procesů, získání konkurenční výhody, zvýšení bezpečnostního povědomí u zaměstnanců, zvýšení informační bezpečnosti ve společnosti nebo identifikace opatření napomáhajících plnění požadavků Obecného nařízení o ochraně osobních údajů.

Cílem práce byl návrh zavedení bezpečnostních opatření pro zvládání největších rizik a zvýšení informační bezpečnosti ve společnosti vyvíjející software.

Vedení společnosti od této práce očekávalo analýzu rizik a návrh bezpečnostních opatření pro zvládání největších rizik, po jejichž implementaci dojde ke zvýšení bezpečnostního povědomí u zaměstnanců a zvýšení informační bezpečnosti ve společnosti.

Cíle práce a očekávání vedení společnosti byly splněny.

SEZNAM POUŽITÉ LITERATURY

[1] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[2] *ČSN ISO/IEC 27000, Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnostní informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, 2014.

[3] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[4] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[5] *ČSN EN ISO 9000, Systémy managementu kvality – Základní principy a slovník*. Praha: Úřad pro technickou normalizaci, 2016.

[6] SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi*. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.

[7] *Building an Information Technology Security Awareness and Training Program: Computer security*. Gaithersburg, U.S.: National Institute of Standards and Technology, 2003.

[8] *ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů.* Praha: Český normalizační institut, 2014.

[9] *ESET Mobile Device Management pro iOS* [online]. b.r. [cit. 2017-05-06]. Dostupné z: https://www.eset.com/cz/firmy/ochrana-dat/mdm-ios/

[10] *VeraCrypt - Documentation* [online]. b.r. [cit. 2017-05-06]. Dostupné z: https://veracrypt.codeplex.com/wikipage?title=Introduction

[11] *Pevný internet - T-Mobile* [online]. b.r. [cit. 2017-05-06]. Dostupné z: https://www.t-mobile.cz/podnikatele-firmy/pevny-internet/

[12] *APC Back-UPS 1400VA (BX1400U-FR)* [online]. b.r. [cit. 2017-05-06]. Dostupné z: https://www.tsbohemia.cz/apc-back-ups-1400va-230v-avr-french-sockets-_d214044.html

[13] *MALPRO EIP 18x13 instalační lišta vkládací, 18x13mm, bílá (RAL 9003), kus = 2m* [online]. b.r. [cit. 2017-05-06]. Dostupné z: https://www.lancomat.cz/eip-18x13-instalacni-lista-vkladaci-18x13mm-bila-ral-9003-kus-2m-p6235/

[14] *ESET Endpoint Security* [online]. b.r. [cit. 2017-05-06]. Dostupné z: https://www.eset.com/cz/firmy/ochrana-dat/windows-security/

[15] *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. In: . Brusel, 2016.

SEZNAM ZKRATEK

IS – Information System

ICT – Information and Communication Technologies

ISMS – Information Security Management System

ITG – IT Governance

ITSM – IT Service Management

IT – Information Technologies

ITIL – Information Technology Infrastructure Library

COBIT – Control Objectives for Information and Related Technology

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

ITU – International Telecommunications Union

OSN – Organizace spojených národů

ČSNI – Český normalizační institut

CEN – European Committee for Standardization

CENELEC – European Committee for Electrotechnical Standardization

ETSI – European Telecommunications Standards Institute

CISO – Chief Information Security Officer

ISACA – Information Systems Audit and Control Association

CISM – Certified Information Security Manager

CISA – Certified Information Systems Auditor

UPS – Uninterruptible Power Supply/Source

SLA – Service Level Agreement

CSIRT – Computer Security Incident Response Team

GDPR – General Data Protection Regulation

SEZNAM TABULEK

Tabulka 1: Srovnávací rámec bezpečnostního vzdělávání (Upraveno dle [7]) 31

Tabulka 2: Hodnota aktiva (Zdroj: vlastní zpracování) 45

Tabulka 3: Ohodnocení aktiv (Zdroj: vlastní zpracování) 45

Tabulka 4: Hodnota hrozby (Zdroj: vlastní zpracování) 46

Tabulka 5: Ohodnocení hrozeb (Zdroj: vlastní zpracování) 47

Tabulka 6: Matice zranitelnosti (Zdroj: vlastní zpracování) 48

Tabulka 7: Hodnota rizika (Zdroj: vlastní zpracování) 49

Tabulka 8: Matice rizik (Zdroj: vlastní zpracování) 50

Tabulka 9: Akceptace rizik (Zdroj: vlastní zpracování) 52

Tabulka 10: Opatření pro zvládání největších rizik (Zdroj: vlastní zpracování) 54

Tabulka 11: Aplikovatelnost navržených opatření (Zdroj: vlastní zpracování) 72

Tabulka 12: Náklady na návrh opatření (Zdroj: vlastní zpracování) 76

Tabulka 13: Náklady na zavedení (údržbu) opatření (Zdroj: vlastní zpracování) 77

Tabulka 14: Náklady na návrh a zavedení opatření (Zdroj: vlastní zpracování) 78

SEZNAM OBRÁZKŮ

Obrázek 1: Vztah úrovní bezpečnosti v organizaci (Upraveno dle [3]) 14

Obrázek 2: Graf přiměřené bezpečnosti za akceptovatelné náklady (Převzato z [4]) 15

Obrázek 3: Model PDCA v ISMS (Převzato z [4]) 18

Obrázek 4: Model ITG (Převzato z [3])..... 19

Obrázek 5: Vztah ITG a ITSM (Převzato z [3]) 20

Obrázek 6: COBIT kostka (Převzato z [3]) 22

Obrázek 7: Řada norem ISO/IEC 27000 (Převzato z [3]) 24

Obrázek 8: Oblasti ISMS dle přílohy A normy ISO/IEC 27002 (Upraveno dle [8]) 33

Obrázek 9: Proces vývoje velké verze produktu (Zdroj: vlastní zpracování)..... 35

Obrázek 10: Proces prodeje (Zdroj: vlastní zpracování) 35

Obrázek 11: Proces implementace (Zdroj: vlastní zpracování)..... 36

Obrázek 12: Proces prodeje PPÚ (Zdroj: vlastní zpracování)..... 36

Obrázek 13: Proces technické podpory (Zdroj: vlastní zpracování)..... 37

Obrázek 14: Proces změny v produktu (Zdroj: vlastní zpracování) 37

Obrázek 15: Proces prodeje (obnovy) maintenance (Zdroj: vlastní zpracování) 37

Obrázek 16: Proces prodeje (navýšení) licence (Zdroj: vlastní zpracování) 38

Obrázek 17: Ukázka vytvoření svazku VeraCrypt (Zdroj: vlastní zpracování) 64

Obrázek 18: Ukázka možností šifrování svazku VeraCrypt (Zdroj: vlastní zpracování)65

Obrázek 19: Redundantního internetového připojení (Převzato z [11])..... 66

Obrázek 20: Zdroj nepřerušovaného napájení APC BX1400U (Převzato z [12])..... 66

Obrázek 21: MALPRO EIP 18x13 instalační lišta vkládací (Převzato z [13]) 67

Obrázek 22: Ukázka prostředí ESET Endpoint Security (Převzato z [14])..... 69

SEZNAM PŘÍLOH

PŘÍLOHA Č. 1: OHODNOCENÍ AKTIV……..……...I

PŘÍLOHA Č. 2: MATICE ZRANITELNOSTI.....II

PŘÍLOHA Č. 3: MATICE RIZIK…….....III

PŘÍLOHA Č. 4: NÁVRŽENÁ OPATŘENÍ…….…...IV

PŘÍLOHA Č. 5: PROHLÁŠENÍ O APLIKOVATELNOSTI……...…V

PŘÍLOHA Č. 1: OHODNOCENÍ AKTIV

Aktivum (A)	Zdroj	Dostupnost	Důvěrnost	Integrita	Hodnota aktiva
Obchodní procesy a činnosti					
obchodní procesy a činnosti	servery, databázový systém (SQL)	4	5	5	5
Informace					
interní data	servery, databázový systém (SQL)	4	5	5	5
data zákazníků	servery, databázový systém (SQL)	3	5	4	4
zdrojové kódy	servery	4	5	4	4
zálohy	servery	5	5	5	5
Hardware					
servery	servery	5	4	5	5
klientské počítače	pracovní stanice, přenosné počítače	3	3	2	3
procesní periferie	tiskárny, telefony, přenosná úložiště	4	3	2	3
Software					
serverový operační systém	servery	5	4	4	4
databázový systém (SQL)	servery	4	4	5	4
informační systém	servery	5	4	5	5
klientský operační systém	pracovní stanice, přenosné počítače	3	2	2	2
Sítě					
síťová infrastruktura	síťové prvky, kabeláž	4	4	4	4
Služby					
elektrická energie	dodavatel elektrické energie	5	3	4	4
internetové připojení	poskytovatel internetového připojení	4	4	4	4
vzdálené připojení (VPN)	síťová infrastruktura, interní IT	4	4	4	4
servis, údržba, profylaxe	interní IT	3	2	2	2

PŘÍLOHA Č. 2: MATICE ZRANITELNOSTI

Zranitelnost (V)		Aktivum	Obchodní procesy a činnosti	obchodní procesy a činnosti	Informace	interní data	data zákazníků	zdrojové kódy	zálohy	Hardware	servery	klientské počítače	procesní periferie	Software	serverový operační systém	databázový systém (SQL)	informační systém	klientský operační systém	Sítě	síťová infrastruktura	Služby	elektrická energie	internetové připojení	vzdálené připojení (VPN)	servis, údržba, profylaxe
		A		5		5	4	4	5		5	3	3		4	4	5	2		4		4	4	4	2
Hrozba	**T**																								
Fyzické poškození																									
Požár	2								2		2	1	1							2		2	1		1
Poškození vodou	2								2		2	1								2		3	2		2
Znečištění	3										2	2								1					3
Zničení zařízení nebo médií	2								2		1	1	1							1		2	2		2
Ztráta základních služeb																									
Selhání klimatizace nebo dodávky vody	2								1		2									1					2
Přerušení dodávky elektřiny	3										5	3	3							3		5	5		4
Selhání internetového připojení	4										3	2	1							2			5	4	3
Ohrožení informací																									
Vzdálená špionáž	2			3		3	2	3	2						1	1	1	3							
Krádež médií nebo dokumentů	2			3		2	2	1	2			1	3			2	2	1							
Krádež zařízení	2												2							1		1	1		
Zprovoznění recyklovaných nebo vyřazených médií	1			3		2	1	2	3																1
Data pocházející z nedůvěryhodných zdrojů	3											1	1			1	1	1							
Falšování pomocí technického vybavení	3										2	2	2							2			3		2
Falšování pomocí aplikačního progr. vybavení	3														2	2	2	2					1	2	
Technická selhání																									
Chybné fungování zařízení	3										4	2	3							1		2	2	2	3
Chybné fungování aplikačního progr. vybavení	3														4	3	3	1		1			1		
Chyba údržby	2								2		2	2	2		3	1	1	1		2		1	1		5
Neoprávněné činnosti (vnitřní)																									
Neoprávněné použití zařízení	2			3		4	3	3	1		2	4	2							3			2		
Podvodné kopírování aplikačního progr. vybavení	2														2	2	1	2							
Poškození dat	3			2		4	3	4	5						2	4	3	1							
Nezákonné zpracování dat	1			4		5	4	3	4						1	5	4	2							
Neoprávněné činnosti (vnější)																									
Neoprávněné použití zařízení	2			3		4	3	3	1		3	3	3							3					
Podvodné kopírování aplikačního progr. vybavení	3														2	2	1	2							
Poškození dat	2			2											2	2	1	2							
Nezákonné zpracování dat	2			4		4	3	4	5						2	4	3	1							
Ohrožení funkčnosti																									
Chyba v používání	2					5	5	3	4		2	3	3		4	4	4	2		2		2	2		2
Zneužití oprávnění	3			3		3	3	3	2		2	2	1		3	3	2	2		2			2		

PŘÍLOHA Č. 3: MATICE RIZIK

Riziko (R)		Aktivum	Obchodní procesy a činnosti	obchodní procesy a činnosti	Informace	interní data	data zákazníků	zdrojové kódy	zálohy	Hardware	servery	klientské počítače	procesní periferie	Software	serverový operační systém	databázový systém (SQL)	informační systém	klientský operační systém	Sítě	síťová infrastruktura	Služby	elektrická energie	internetové připojení	vzdálené připojení (VPN)	servis, údržba, profylaxe
		A		5		5	4	4	5		5	3	3		4	4	5	2		4		4	4	4	2
Hrozba	**T**																								
Fyzické poškození																									
Požár	2								20		20	6	6							16		16	8		4
Poškození vodou	2								20		20	6								16		24	16		8
Znečištění	3										30	18								12					18
Zničení zařízení nebo médií	2								20		10	6	6							8		16	16		8
Ztráta základních služeb																									
Selhání klimatizace nebo dodávky vody	2								10		20									8					8
Přerušení dodávky elektřiny	3										75	27	27							36		60	60		24
Selhání internetového připojení	4										60	24	12							32			80	64	24
Ohrožení informací																									
Vzdálená špionáž	2			30		30	16	24	20						8	8	10	12							
Krádež médií nebo dokumentů	2			30		20	16	8	20			6	18			16	20	4							
Krádež zařízení	2												12							8		8	8		
Zprovoznění recyklovaných nebo vyřazených médií	1			15		10	4	8	15																2
Data pocházející z nedůvěryhodných zdrojů	3											9	9			12	15	6							
Falšování pomocí technického vybavení	3										30	18	18							24			36		12
Falšování pomocí aplikačního progr. vybavení	3														24	24	30	12					12	24	
Technická selhání																									
Chybné fungování zařízení	3										60	18	27							12		24	24	24	18
Chybné fungování aplikačního progr. vybavení	3														48	36	45	6		12			12		
Chyba údržby	2								20		20	12	12		24	8	10	4		16		8	8		20
Neoprávněné činnosti (vnitřní)																									
Neoprávněné použití zařízení	2			30		40	24	24	10		20	24	12							24			16		
Podvodné kopírování aplikačního progr. vybavení	2														16	16	10	8							
Poškození dat	3			30		60	36	48	75						24	48	45	6							
Nezákonné zpracování dat	1			20		25	16	12	20						4	20	20	4							
Neoprávněné činnosti (vnější)																									
Neoprávněné použití zařízení	2			30		40	24	24	10		30	18	18							24					
Podvodné kopírování aplikačního progr. vybavení	3														24	24	15	12							
Poškození dat	2			20											16	16	10	8							
Nezákonné zpracování dat	2			40		40	24	32	50						16	32	30	4							
Ohrožení funkčnosti																									
Chyba v používání	2					50	40	24	40		20	18	18		32	32	40	8		16		16	16		8
Zneužití oprávnění	3			45		45	36	36	30		30	18	9		36	36	30	12		24			24		

PŘÍLOHA Č. 4: NÁVRŽENÁ OPATŘENÍ

Hrozba (T)	Bezpečnostní opatření	Rozhodnutí
Fyzické poškození		
Požár	A.11.1.4, A.17.2.1	NEZAVÁDĚT
Poškození vodou	A.11.1.4, A.17.2.1	NEZAVÁDĚT
Znečištění	A.11.2.1., A 11.2.4, A.17.2.1	NEZAVÁDĚT
Zničení zařízení nebo médií	A.11.1.3, A 11.2.1, A.11.2.4, A.11.2.6, A.17.2.1	NEZAVÁDĚT
Ztráta základních služeb		
Selhání klimatizace nebo dodávky vody	A.11.2.2, A.11.2.4	NEZAVÁDĚT
Přerušení dodávky elektřiny	A.11.2.2, A.11.2.3, A.17.2.1	ZAVÉST
Selhání internetového připojení	A.11.2.2, A.11.2.3, A.17.2.1	ZAVÉST
Ohrožení informací		
Vzdálená špionáž	A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.4, A.9.4.5, A.10.1.1, A.10.1.2, A.11.2.6, A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.6.2, A.14.1.2, A.14.1.3	NEZAVÁDĚT
Krádež médií nebo dokumentů	A.6.2.1, A.6.2.2, A.7.2.3, A.7.3.1, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.4.1, A.10.1.1, A.10.1.2, A.11.1.1, A.11.1.2, A.11.1.3, A.11.2.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.1, A.13.2.2, A.13.2.3, A.14.1.2, A.14.1.3, A.14.2.5	NEZAVÁDĚT
Krádež zařízení	A.6.2.1, A.6.2.2, A.7.2.3, A.7.3.1, A.10.1.1, A.10.1.2, A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.2.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.17.2.1	NEZAVÁDĚT
Zprovoznění recyklovaných nebo vyřazených médií	A.8.3.2, A.10.1.1, A.10.1.2, A.11.2.7	NEZAVÁDĚT
Data pocházející z nedůvěryhodných zdrojů	A.12.1.4, A.12.6.2, A.13.1.1, A.13.2.1, A.13.2.2, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3	NEZAVÁDĚT
Falšování pomocí technického vybavení	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.5, A.11.2.8	NEZAVÁDĚT
Falšování pomocí aplikačního progr. vybavení	A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.12.2.1, A.11.2.6, A.11.2.9, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.6.2, A.13.1.1, A.14.2.4, A.14.2.5	NEZAVÁDĚT
Technická selhání		
Chybné fungování zařízení	A.11.1.4, A.11.2.1, A.11.2.4, A.11.2.5, A.11.2.8, A.17.2.1	ZAVÉST
Chybné fungování aplikačního progr. vybavení	A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4	ZAVÉST
Chyba údržby	A.11.2.2, A.11.2.4, A.12.3.1	NEZAVÁDĚT
Neoprávněné činnosti (vnitřní)		
Neoprávněné použití zařízení	A.9.1.2, A.9.2.5, A.9.2.6, A.9.4.1 A.11.1.1, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8, A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4	ZAVÉST
Podvodné kopírování aplikačního progr. vybavení	A.7.2.3, A.11.2.8, A.12.5.1, A.14.2.4	NEZAVÁDĚT
Poškození dat	A.9.1.2, A.9.4.1, A.11.2.8, A.12.2.1, A.12.3.1, A.14.1.3	ZAVÉST
Nezákonné zpracování dat	A.10.1.1, A.10.1.2, A.11.2.8, A.11.2.9, A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.1, A.13.2.2, A.13.2.3, A.14.1.2, A.14.1.3	NEZAVÁDĚT
Neoprávněné činnosti (vnější)		
Neoprávněné použití zařízení	A.9.1.2, A.9.2.5, A.9.2.6, A.9.4.1 A.11.1.1, A.11.1.3, A.11.2.1, A.11.2.6, A.11.2.8, A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4	ZAVÉST
Podvodné kopírování aplikačního progr. vybavení	A.7.2.3, A.11.2.8, A.12.5.1, A.14.2.4	NEZAVÁDĚT
Poškození dat	A.9.1.1, A.9.1.2, A.9.4.1, A.11.2.8,A.12.3.1, A.12.2.1, A.12.6.2, A.14.1.3	NEZAVÁDĚT
Nezákonné zpracování dat	A.10.1.1, A.10.1.2, A.11.2.8, A.11.2.9, A.12.2.1, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.1, A.13.2.2, A.13.2.3, A.14.1.2, A.14.1.3	ZAVÉST
Ohrožení funkčnosti		
Chyba v používání	A.6.2.1, A.7.2.2, A.8.1.3, A.8.2.3, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9	ZAVÉST
Zneužití oprávnění	A.7.2.3, A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.3, A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4	ZAVÉST

PŘÍLOHA Č. 5: PROHLÁŠENÍ O APLIKOVATELNOSTI

A.5 Politiky bezpečnosti informací

A.5.1 Směřování bezpečnosti informací vedením organizace

Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.

A.5.1.1 Politiky pro bezpečnost informací

Opatření: Soubor politik pro bezpečnost informací musí být definován, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.

Vyloučeno: Ano

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Opatření: Pro zjištění neustálé vhodnosti, přiměřenosti a efektivnosti musí být politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech vždy, když nastane významná změna.

Vyloučeno: Ano

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustavit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Opatření: Musí být definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Příručka ISMS.

A.6.1.2 Princip oddělení povinností

Opatření: Pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení neslučitelných povinností a odpovědností.

Vyloučeno: Ne

Způsob plnění požadavku: Dokument s popisem pracovních pozic (role, práva, povinnosti, odpovědnosti) a patřičné nastavení v Active Directory.

A.6.1.3 Kontakt s příslušnými orgány a autoritami

Opatření: Musí být udržovány přiměřené vztahy s příslušnými orgány a autoritami.

Vyloučeno: Ne

Způsob plnění požadavku: Odebírání novinek z webových stránek Národního centra kybernetické bezpečnosti (www.govcert.cz) nebo Národního CSIRT České republiky (www.csirt.cz).

A.6.1.4 Kontakt se zájmovými skupinami

Opatření: Musí být udržovány přiměřené vztahy s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími.

Vyloučeno: Ne

Způsob plnění požadavku: Členství v odborných fórech nebo účast na konferencích o bezpečnosti.

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Bezpečnost informací musí být zohledněna v řízení projektů nezávisle na typu projektu.

Vyloučeno: Ne

Způsob plnění požadavku: Řízení projektů na základě nejnovějších norem a doporučení v oblasti bezpečnosti informací.

A.6.2 Mobilní zařízení a práce na dálku.

Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.

A.6.2.1 Politika mobilních zařízení

Opatření: Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.

Vyloučeno: Ne

Způsob plnění požadavku: Politika mobilních zařízení, software ESET Mobile Device Management se vzdálenou správou.

A.6.2.2 Práce na dálku

Opatření: Musí být implementována politika a relevantní bezpečnostní opatření na ochranu informací, které jsou přístupné, zpracované nebo ukládané v místech pro práci na dálku.

Vyloučeno: Ano

A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.

A.7.1.1 Prověřování

Opatření: Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků, týkajících se činnosti organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potenciálních rizik.

Vyloučeno: Ano

A.7.1.2 Podmínky pracovního vztahu

Opatření: Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací.

Vyloučeno: Ano

A.7.2 Během pracovního vztahu

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.

A.7.2.1 Odpovědnosti vedení organizace

Opatření: Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustanovenými politikami a postupy v organizaci.

Vyloučeno: Ano

A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací

Opatření: Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany, musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Zavedení plánu vzdělávání zaměstnanců, pravidelné hromadné e-maily s bezpečnostní tématikou.

A.7.2.3 Disciplinární řízení

Opatření: Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Příručka ISMS.

A.7.3 Ukončení a změna pracovního vztahu

Cíl: Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu.

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu

Opatření: Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné po ukončení nebo změně pracovního vztahu, musí být definovány, komunikovány se zaměstnanci nebo smluvními stranami a prosazovány.

Vyloučeno: Ano

A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.

A.8.1.1 Seznam aktiv

Opatření: Aktiva související s informacemi a vybavení pro zpracování informací musí být identifikována a seznam těchto aktiv musí být vytvořen a udržován aktuální.

Vyloučeno: Ano

A.8.1.2 Vlastnictví aktiv

Opatření: Aktiva udržovaná v seznamu musí mít určeného vlastníka.

Vyloučeno: Ano

A.8.1.3 Přípustné použití aktiv

Opatření: Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací.

Vyloučeno: Ne

Způsob plnění požadavku: Dokument definující přípustné použití aktiv.

A.8.1.4 Navrácení aktiv

Opatření: Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci pracovníci externích stran odevzdat veškerá jim svěřená aktiva, která jsou majetkem organizace.

Vyloučeno: Ano

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.

A.8.2.1 Klasifikace informací

Opatření: Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci.

Vyloučeno: Ano

A.8.2.2 Označování informací

Opatření: Pro označování informací musí být vytvořen a implementován vhodný soubor postupů, které jsou v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ano

A.8.2.3 Manipulaci s aktivy

Opatření: Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ne

Způsob plnění požadavku: Dokument definující manipulaci s aktivy.

A.8.3 Manipulace s médii

Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.

A.8.3.1 Správa výměnných médií

Opatření: Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatým organizací.

Vyloučeno: Ano

A.8.3.2 Likvidace médií

Opatření: Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.

Vyloučeno: Ano

A. 8.3.3 Přeprava fyzických médií

Opatření: Média obsahující informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.

Vyloučeno: Ano

A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a vybavení pro zpracování informací.

A.9.1.1 Politika řízení přístupu

Opatření: Musí být ustanovena, dokumentována a přezkoumávána politika řízení přístupu v závislosti na požadavcích na činnosti organizace a bezpečnosti informací.

Vyloučeno: Ano

A.9.1.2 Přístup k sítím a síťovým službám

Opatření: Uživatelé musí mít přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli zvlášť oprávnění.

Vyloučeno: Ano

A.9.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.

A.9.2.1 Registrace a zrušení registrace uživatele

Opatření: Pro přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.

Vyloučeno: Ano

A.9.2.2 Správa uživatelských přístupů

Opatření: Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám musí být implementován formalizovaný proces správy uživatelských přístupů.

Vyloučeno: Ano

A.9.2.3 Správa privilegovaných přístupových práv

Opatření: Musí být omezeno a řízeno přidělování a používání privilegovaných přístupových práv.

Vyloučeno: Ne

Způsob plnění požadavku: Dokument definující správu privilegovaných přístupových práv. Schvalovací proces je realizován pomocí interního systému pro řízení požadavků a služeb.

A.9.2.4 Správa tajných autentizačních informací uživatelů

Opatření: Přidělování tajných autentizačních informací musí být řízeno formalizovaným procesem.

Vyloučeno: Ano

A.9.2.5 Přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.

Vyloučeno: Ne

Způsob plnění požadavku: Za přezkoumávání přístupových práv uživatelů jsou zodpovědní vlastníci aktiv.

A.9.2.6 Odebrání nebo úprava přístupových práv

Opatření: Při ukončení nebo změně pracovního vztahu, smluvního vztahu nebo dohody musí být všem zaměstnancům a externím stranám odejmuta nebo pozměněna přístupová práva k informacím a vybavení pro zpracování informací.

Vyloučeno: Ano

A.9.3 Odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.

A.9.3.1 Používání tajných autentizačních informací

Opatření: Při používání tajných autentizačních informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.

Vyloučeno: Ne

Způsob plnění požadavku: Pracovní smlouva, směrnice k uživatelským účtům.

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Opatření: V souladu s politikou řízení přístupu musí být omezen přístup k informacím a funkcím aplikace.

Vyloučeno: Ne

Způsob plnění požadavku: Dokument s popisem pracovních pozic (role, práva, povinnosti, odpovědnosti) a patřičné nastavení v Active Directory.

A.9.4.2 Bezpečné postupy přihlášení

Opatření: Pokud to politika řízení přístupu vyžaduje, musí být přístup k systémům a aplikacím řízen postupy bezpečného přihlášení.

Vyloučeno: Ano

A.9.4.3 Systém správy hesel

Opatření: Systémy správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.

Vyloučeno: Ano

A.9.4.4 Použití privilegovaných programových nástrojů

Opatření: Musí být omezeno a přísně kontrolováno použití programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly.

Vyloučeno: Ano

A.9.4.5 Řízení přístupu ke zdrojovým kódům

Opatření: Musí být omezen přístup ke zdrojovým kódům programů.

Vyloučeno: Ano

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit řádné a efektivní používání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací.

A.10.1.1 Politika pro použití kryptografických opatření

Opatření: Musí být vytvořena a implementována politika pro užívání kryptografických opatření na ochranu informací.

Vyloučeno: Ne

Způsob plnění požadavku: Dokument definující kryptografii, softwarový nástroj VeraCrypt.

A.10.1.2 Správa klíčů

Opatření: Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.

Vyloučeno: Ano

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Bezpečnost oblasti

Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: Bezpečnostní perimetry musí být definovány a používány k ochraně oblastí, které obsahují citlivé nebo kritické informace a vybavení pro zpracování informací.

Vyloučeno: Ano

A.11.1.2 Fyzické kontroly vstupu

Opatření: Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.

Vyloučeno: Ano

Způsob plnění požadavku: kontrola na recepci; autentizace pomocí vstupních karet; při vstupu k prvkům umístěným v datovém centru jsou přísné kontroly vstupu

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Opatření: Musí být navržena a aplikována fyzická bezpečnost kanceláří, místností a vybavení.

Vyloučeno: Ano

A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí

Opatření: Musí být navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.

Vyloučeno: Ano

A.11.1.5 Práce v bezpečných oblastech

Opatření: Musí být navrženy a aplikovány postupy pro práci v bezpečných oblastech.

Vyloučeno: Ano

A.11.1.6 Oblasti pro nakládku a vykládku

Opatření: Přístupové body, jako oblasti pro nakládku a vykládku a další místa, kde se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolovány, a pokud je to možné, izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu k nim.

Vyloučeno: Ano

A.11.2 Zařízení

Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.

A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

Vyloučeno: Ano

A.11.2.2 Podpůrné služby

Opatření: Zařízení musí být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

Vyloučeno: Ne

Způsob plnění požadavku: Zřízení redundantního internetového připojení, zajištění údržby již implementovaného zdroje nepřerušovaného napájení (dokument s popisem pracovních pozic – správce informačních technologií).

A.12.2.3 Bezpečnost kabelových rozvodů

Opatření: Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlechem, rušením či poškozením.

Vyloučeno: Ne

Způsob plnění požadavku: Kabelážní lišty.

A.11.2.4 Údržba zařízení

Opatření: Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

Vyloučeno: Ano

A.11.2.5 Přemístění aktiv

Opatření: Zařízení, informace nebo software nesmí být přemísťováno mimo prostory organizace bez předchozího schválení.

Vyloučeno: Ano

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: Aktiva mimo prostory organizace musí být zabezpečena s přihlédnutím k rozdílným rizikům, která vyplívají z jejich použití mimo organizaci.

Vyloučeno: Ano

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Opatření: Všechny prvky zařízení obsahující paměťová média musí být zkontrolovány tak, aby bylo zajištěno, že před jejich likvidací nebo opakovaným použitím budou jakákoliv citlivá data a licencovaný software odstraněny nebo bezpečně přepsány.

Vyloučeno: Ano

A.11.2.8 Uživatelská zařízení bez obsluhy

Opatření: Uživatelé musí zajistit přiměřenou ochranu zařízení bez obsluhy.

Vyloučeno: Ne

Způsob plnění požadavku: Směrnice k uživatelským účtům.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Musí být přijata zásada prázdného stolu ve vztahu k dokumentům a výměnným paměťovým médiím a zásad prázdné obrazovky monitoru u vybavení pro zpracování informací.

Vyloučeno: Ne

Způsob plnění požadavku: Směrnice k uživatelským účtům.

A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.

A.12.1.1 Dokumentované provozní postupy

Opatření: Provozní postupy musí být dokumentovány a musí být dostupné uživatelům podle potřeby.

Vyloučeno: Ano

A.12.1.2 Řízení změn

Opatření: Změny v organizaci a jejích procesech, v prostředích pro zpracování informací a systémech, které ovlivňují bezpečnost informací, musí být řízeny.

Vyloučeno: Ano

A.12.1.3 Řízení kapacit

Opatření: Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.

Vyloučeno: Ano

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Opatření: Pro snížení rizika neoprávněného přístupu nebo změn provozního prostředí musí být odděleno prostředí vývoje, testování a provozu.

Vyloučeno: Ano

A.12.2 Ochrana proti malwaru

Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru.

A.12.2.1 Opatření proti malwaru

Opatření: Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.

Vyloučeno: Ne

Způsob plnění požadavku: Bezpečnostní řešení ESET Endpoint Security se vzdálenou správou, vzdělávání zaměstnanců v oblasti informační bezpečnosti (bezpečnostní povědomí).

A.12.3 Zálohování

Cíl: Chránit proti ztrátě dat.

A.12.3.1 Zálohování informací

Opatření: Záložní kopie informací, softwaru a binárních obrazů systému musí být pořizovány v pravidelných intervalech v souladu se schválenou politikou zálohování.

Vyloučeno: Ne

Způsob plnění požadavku: Směrnice k zálohování dat s požadavky na zálohování (co zálohovat, kam zálohovat, jak často zálohovat, šifrování, testování obnovy záloh atd.).

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a vytvářet záznamy.

A.12.4.1 Zaznamenávání událostí formou logů

Opatření: Musí být pořizovány, uchovávány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.

Vyloučeno: Ne

Způsob plnění požadavku: Směrnice k zaznamenávání definující logování aktivity uživatelů, selhání, události bezpečnosti informací, přístupy atd.). Nákup potřebného software, hardware a obsazení pracovní pozice pro datového analytika.

A.12.4.2 Ochrana logů

Opatření: Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.

Vyloučeno: Ano

A.12.4.3 Logy o činnosti administrátorů a operátorů

Opatření: Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.

Vyloučeno: Ano

A.12.4.4 Synchronizace hodin

Opatření: Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.

Vyloučeno: Ano

A.12.5 Správa provozního softwaru

Cíl: Zajistit integritu provozních systémů.

A.12.5.1 Instalace softwaru na provozní systémy

Opatření: Musí být implementovány postupy řízené instalace softwaru na provozních systémech.

Vyloučeno: Ano

A.12.6 Řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.1 Řízení technických zranitelností

Opatření: Musí být zajištěno včasné získání informací o existenci technických zranitelností provozovaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na zvládání souvisejících rizik.

Vyloučeno: Ano

A.12.6.2 Omezení instalace softwaru

Opatření: Musí být ustanovena a implementována pravidla ohledně instalace softwaru uživateli.

Vyloučeno: Ano

A.12.7 Hlediska auditu informačních systémů

Cíl: Minimalizovat dopady auditních činností na provozní systémy.

A.12.7.1 Opatření k auditu informačních systémů

Opatření: Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesů organizace.

Vyloučeno: Ano

A.13 Bezpečnost komunikací

A.13.1 Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.

A.13.1.1 Opatření v sítích

Opatření: K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.

Vyloučeno: Ano

A.13.1.2 Bezpečnost síťových služeb

Opatření: Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb, ať už jsou zajišťovány interně nebo cestou outsourcingu.

Vyloučeno: Ano

A.13.1.3 Princip oddělení v sítích

Opatření: V sítích musí být odděleny skupiny informačních služeb, uživatelů a informačních systémů.

Vyloučeno: Ano

A.13.2 Přenos informací

Cíl: Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.

A.13.2.1 Politiky a postupy při přenosu informací

Opatření: Musí existovat formalizované politiky, postupy a opatření k ochraně přenosu informací pomocí jakéhokoliv typu komunikačního vybavení.

Vyloučeno: Ano

A.13.2.2 Dohody o přenosu informací

Opatření: Dohody se musí zabývat zabezpečeným přenosem informací týkající se činností organizace mezi organizací a externími stranami.

Vyloučeno: Ano

A.13.2.3 Elektronické předávání zpráv

Opatření: Musí být vhodným způsobem chráněny elektronicky přenášené informace.

Vyloučeno: Ano

A.13.2.4 Dohody o utajení nebo mlčenlivosti

Opatření: Musí být identifikovány, pravidelně přezkoumávány a dokumentovány požadavky na dohody o utajení nebo na dohody o mlčenlivosti reflektující potřeby organizace na ochranu informací.

Vyloučeno: Ano

A.14 Akvizice, vývoj a údržba systémů

A.14.1 Bezpečnostní požadavky informačních systémů

Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.

A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací

Opatření: V požadavcích na nové informační systémy nebo na rozšíření existujících systémů musí být obsaženy také požadavky týkající se bezpečnosti informací.

Vyloučeno: Ano

A.14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích

Opatření: Informace přenášené ve veřejných sítích v rámci aplikačních služeb musí být chráněny před podvodnými aktivitami, zpochybňováním smluv, neoprávněným vyzrazením a modifikací.

Vyloučeno: Ano

A.14.1.3 Ochrana transakcí aplikačních služeb

Opatření: Musí být zajištěna ochrana informací přenášených při transakcích aplikačních služeb tak, aby se zabránilo neúplnému přenosu informací, chybnému směrování, neoprávněné změně zpráv, neoprávněnému vyzrazení, neoprávněné duplikaci nebo opakování přenosu zpráv.

Vyloučeno: Ano

A.14.2 Bezpečnost v procesech vývoje a podpory

Cíl: Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů.

A.14.2.1 Politika bezpečného vývoje

Opatření: Musí být ustanovena v rámci organizace aplikována pravidla pro vývoj softwaru a systémů.

Vyloučeno: Ano

A.14.2.2 Postupy řízení změn systému

Opatření: Pomocí formalizovaných postupů řízení změn musí být řízeny změny systémů v rámci jejich životního cyklu vývoje.

Vyloučeno: Ano

A.14.2.3 Technické přezkoumání aplikací po změnách provozní platformy

Opatření: V případě změny provozní platformy musí být přezkoumány a otestovány aplikace kritické pro činnost organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.

Vyloučeno: Ano

A.14.2.4 Omezení změn softwarových balíků

Opatření: Modifikace softwarových balíků musí být omezeny na nezbytné změny a veškeré provádění změny musí být přísně řízeny.

Vyloučeno: Ano

A.14.2.5 Principy budování bezpečných systémů

Opatření: Principy budování bezpečných systémů musí být ustanoveny, dokumentovány, udržovány a aplikovány při implementaci informačních systémů.

Vyloučeno: Ano

A.14.2.6 Prostředí bezpečného vývoje

Opatření: Pro vývoj systémů a jejich integraci, pokrývající celý životní cyklus vývoje systémů, musí organizace vytvořit a přiměřeně chránit prostředí bezpečného vývoje systémů.

Vyloučeno: Ano

A.14.2.7 Outsourcovaný vývoj

Opatření: Organizace musí dohlížet a monitorovat činnosti outsourcovaného vývoje systému.

Vyloučeno: Ano

A.14.2.8 Testování bezpečnosti systému

Opatření: Během vývoje musí být prováděno testování funkčnosti bezpečnosti.

Vyloučeno: Ano

A.14.2.9 Testování akceptace systémů

Opatření: Pro nové informační systémy, aktualizace a nové verze musí být ustanoveny testovací postupy a odpovídající kritéria a akceptace.

Vyloučeno: Ano

A.14.3 Data pro testování

Cíl: Zajistit ochranu dat používaných pro testování.

A.14.3.1 Ochrana dat pro testování

Opatření: Data pro testování musí být pečlivě vybrána, chráněna a kontrolována.

Vyloučeno: Ano

A.15 Dodavatelské vztahy

A.15.1 Bezpečnost informací v dodavatelských vztazích

Cíl: Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup.

A.15.1.1 Politika bezpečnosti informací pro dodavatelské vztahy

Opatření: Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být odsouhlaseny s dodavateli a dokumentovány.

Vyloučeno: Ano

A.15.1.2 Bezpečnostní požadavky v dohodách s dodavateli

Opatření: Všechny požadavky relevantní bezpečnosti informací musí být ustanoveny a odsouhlaseny s každým dodavatelem, který může přistupovat k informacím organizace, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury.

Vyloučeno: Ano

A.15.1.3 Dodavatelský řetězec informačních a komunikačních technologií

Opatření: Dohody s dodavateli musí zahrnovat požadavky na rizika bezpečnosti informací spojená s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií.

Vyloučeno: Ano

A.15.2 Řízení dodávek služeb dodavatelů

Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.

A.15.2.1 Monitorování a přezkoumávání služeb dodavatelů

Opatření: Organizace musí pravidelně monitorovat, přezkoumávat a auditovat dodávky služeb dodavatelů.

Vyloučeno: Ano

A.15.2.2 Řízení změn ve službách dodavatelů

Opatření: Změny v poskytování služeb dodavateli, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, musí být řízeny s ohledem na kritičnost informací, systémů a procesů organizace, které jsou součástí těchto změn, a s ohledem na opakované posouzení rizik.

Vyloučeno: Ano

A.16 Řízení incidentů bezpečnosti informací

A.16.1 Řízení incidentů bezpečnosti informací a zlepšování

Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst.

A.16.1.1 Odpovědnosti a postupy

Opatření: Pro zajištění rychlé, efektivní a systematické reakce na incidenty bezpečnosti informací musí být ustaveny odpovědnosti a postupy pro zvládání incidentů bezpečnosti informací.

Vyloučeno: Ano

A.16.1.2 Hlášení událostí bezpečnosti informací

Opatření: Události bezpečnosti informací musí být co nejrychleji hlášeny příslušnými řídícími kanály.

Vyloučeno: Ano

A.16.1.3 Hlášení slabých míst bezpečnosti informací

Opatření: Po zaměstnancích a smluvních stranách používající informační systémy a služby musí být vyžadováno, aby si všímali a hlásili jakákoliv slabá místa bezpečnosti informací v systémech nebo službách nebo podezření na ně.

Vyloučeno: Ano

A.16.1.4 Posouzení a rozhodnutí o událostech bezpečnosti informací

Opatření: Události bezpečnosti informací musí být posouzeny a musí být rozhodnuto, zda mají být klasifikovány jako incidenty bezpečnosti informací.

Vyloučeno: Ano

A.16.1.5 Reakce na incidenty bezpečnosti informací

Opatření: Reakce na incidenty bezpečnosti informací musí být v souladu s dokumentovanými postupy.

Vyloučeno: Ano

A.16.1.6 Ponaučení z incidentů bezpečnosti informací

Opatření: Znalosti získané z analýzy a řešení incidentů bezpečnosti informací musí být použity ke snížení pravděpodobnosti nebo dopadu následných incidentů.

Vyloučeno: Ano

A.16.1.7 Shromažďování důkazů

Opatření: Organizace musí definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování informací, které můžou sloužit jako důkazy.

Vyloučeno: Ano

A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

A.17.1 Kontinuita bezpečnosti informací

Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činnost organizace.

A.17.1.1 Plánování kontinuity bezpečnosti informací

Opatření: Organizace musí určit svoje požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací při nepříznivých situacích, například během krizí, katastrof nebo

havárií.

Vyloučeno: Ano

A.17.1.2 Implementace kontinuity bezpečnosti informací

Opatření: Organizace musí ustavit, dokumentovat, implementovat a udržovat procesy, postupy a opatření k zajištění požadované úrovně kontinuity pro bezpečnost informací během nepříznivých situací.

Vyloučeno: Ano

A.17.1.3 Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací

Opatření: Organizace musí v pravidelných intervalech verifikovat ustavená a implementovaná opatření kontinuity bezpečnosti informací, aby zajistila, že jsou dostatečná a efektivní během nepříznivých situací.

Vyloučeno: Ano

A.17.2 Redundance

Cíl: Zajistit dostupnost vybavení pro zpracování informací.

A.17.2.1 Dostupnost vybavení pro zpracování informací

Opatření: Vybavení pro zpracování informací musí být implementováno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost.

Vyloučeno: Ano

A.18 Soulady s požadavky

A.18.1 Soulad s právními a smluvními požadavky

Cíl: Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkající se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků.

A.18.1.1 Identifikace odpovídající legislativy a smluvních požadavků

Opatření: Pro každý informační systém a organizace musí být jednoznačně identifikovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, předpisové a smluvní požadavky a způsob, jakým je organizace dodržuje.

Vyloučeno: Ano

A.18.1.2 Ochrana duševního vlastnictví

Opatření: Pro zajištění souladu se zákonnými, předpisovými a smluvními požadavky, které jsou relevantní ochraně duševního vlastnictví a používání proprietárních softwarových produktů, musí být implementovány vhodně postupy.

Vyloučeno: Ano

A.18.1.3 Ochrana záznamů

Opatření: Záznamy musí být chráněny proti ztrátě, zničení, padělání a neautorizovanému přístupu a zveřejnění, a to v souladu se zákonnými, předpisovými a smluvními požadavky a požadavky týkající se činnosti organizace.

Vyloučeno: Ano

A.18.1.4 Soukromí a ochrana osobních údajů

Opatření: Soukromí a ochrana osobních údajů musí být zajištěny v souladu s odpovídající legislativou a s předpisy, pokud je to použitelné.

Vyloučeno: Ano

A.18.1.5 Regulace kryptografických opatření

Opatření: Kryptografická opatření musí být používána v souladu s příslušnými úmluvami, legislativou a předpisy.

Vyloučeno: Ano

A.18.2 Přezkoumání bezpečnosti informací

Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace.

A.18.2.1 Nezávislá přezkoumání bezpečnosti informací

Opatření: Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cílů opatření, jednotlivých opatření, politik, procesů a postupů bezpečnosti informací) musí být nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna.

Vyloučeno: Ano

A.18.2.2 Shoda s bezpečnostními politikami a normami

Opatření: Vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.

Vyloučeno: Ano

A.18.2.3 Přezkoumání technické shody

Opatření: Informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normami bezpečnosti informací organizace.

Vyloučeno: Ano